Markus Neero

TIETOTURVARISKIT JA NIIDEN HALLINTA BYOD-YMPÄRISTÖSSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Neero, Markus
Tietoturvariskit ja niiden hallinta BYOD-ympäristössä
Jyväskylä: Jyväskylän yliopisto, 2020, 40 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Riekkinen, Janne

Informaatioteknologian kuluttajistuminen on synnyttänyt ilmiön, jossa työntekijät käyttävät omia mobiililaitteitaan työntekoon, ajasta ja paikasta riippumatta. Tätä ilmiötä kutsutaan termillä Bring Your Own Device eli BYOD. BYOD ei viittaa pelkästään mobiililaitteiden käyttöön, vaan siihen voi sisältyä myös työntekijöiden käyttämät ohjelmistot ja palvelut. Koska BYOD mahdollistaa työnteon myös työpaikan ulkopuolelta, on työntekijöillä myös aina pääsy organisaation palveluihin ja dataan. BYOD tuottaa paljon hyötyjä niin työntekijöille, kuin myös työnantajille. Se lisää työntekijöiden tuottavuutta, sekä lisää heidän tyytyväisyyttään, itsenäisyyttään ja vapauttaan. Työnantajat saattavat säästää esimerkiksi laitekustannuksissa. BYOD aiheuttaa organisaatioille kuitenkin myös huomattavia tietoturvariskejä. Lähdekirjallisuuden perusteella muun muassa haittaohjelmat, palvelunestohyökkäykset, sosiaalinen manipulointi, laitteiden katoaminen, sekä työntekijöiden huolimaton tai välinpitämätön toiminta ovat tietoturvariskejä, joita organisaatiot kohtaavat BYOD-ympäristössä. Tietoturvauhat saattavat toteutuessaan muun muassa vahingoittaa organisaation järjestelmiä ja estää niiden oikeanlaisen toiminnan, sekä aiheuttaa organisaation datan vuotamisen ulkopuoliselle taholle. Tietoturvariskien hallintaan voidaan kuitenkin käyttää useita eri tietojärjestelmiä ja teknologioita. Mobiililaitehallintajärjestelmät, mobiilisovellushallintajärjestelmät ja mobiilisisällön hallintajärjestelmät ovat esimerkkejä tietojärjestelmistä, joita voidaan käyttää tietoturvauhkien hallintaan BYOD-ympäristössä. Lisäksi markkinoilla on näitä kaikkia eri järjestelmiä yhdisteleviä kokonaisratkaisuja, joita kutsutaan yleisesti yritysten mobiiliuden hallinnaksi. Tämän lisäksi tietoturvauhkia vastaan voidaan puolustautua kontrolloimalla pääsyä tietoverkkoihin, sekä käyttämällä erilaisia virtualisointitekniikoita. Tutkielmassa kuitenkin havaittiin, että kaikissa hallintateknologioissa on rajoitteita, eikä mikään niistä anna täyttä suojaa esimerkiksi kehittyneitä haittaohjelmia vastaan. Tämän tutkielman tarkoitus oli selvittää minkälaisia tietoturvauhkia organisaatiot kohtaavat BYOD-ympäristössä, ja minkälaisilla teknisillä ratkaisuilla niitä voidaan hallita. Tutkielma toteutettiin kirjallisuuskatsauksena ja sen tulokset perustuvat täysin lähdekirjallisuuteen.

Asiasanat: BYOD, tietoturva, mobiililaitehallinta

ABSTRACT

Neero, Markus
Information Security Issues and Mitigation Techniques in BYOD Environment
Jyväskylä: University of Jyväskylä, 2020, 40 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Riekkinen, Janne

Consumerization of IT has given rise to a phenomenon in which employees use their own mobile devices to work, regardless of time and place. This phenomenon is called Bring Your Own Device. BYOD refers not only to the use of mobile devices but may also include software and services used by employees. Since BYOD also allows people to work from outside the workplace, employees always have access to the services and data of the organization. BYOD brings a lot of benefits for both employees and employers. It increases employee productivity and increases their satisfaction, independence and freedom. Employers may save, for example, on equipment costs. However, BYOD also poses significant security risks for organizations. Based on source literature, for example, denial of service attacks, social engineering, device loss, and employees' careless activities are security risks that enterprises face in BYOD environment. Security threats, when implemented, may damage the organization's systems and prevent them from functioning correctly, and cause the organization's data to be exposed to third parties. However, a wide range of information systems and technologies can be used to manage security risks. Mobile device management systems, mobile application management systems, and mobile content management systems are examples of information systems that can be used to manage security threats in BYOD environment. In addition, the market has overall solutions combining all the different systems, commonly referred to as enterprise mobility management. In addition, security threats can be defended by network access control and using a variety of virtualization technologies. However, the thesis found that all management technologies have limitations and none of them provide full protection against, for example, advanced malware. The purpose of this paper was to identify the types of security threats that organizations face in the BYOD environment and find out what technical solutions can be used to manage them. The thesis was conducted as a literature review and its results are based entirely on literature.

Keywords: BYOD, Information Security, Mobile Device Management

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Työelämä on muuttunut paljon vuosien varrella. Nykyään työntekijät tulevat työpaikalleen mukanaan omat henkilökohtaiset laitteensa ja odottavat, että he voivat hyödyntää niitä myös työnteossaan (Thomson, 2012). Tämä on osa informaatioteknologian kuluttajistumista ja se on synnyttänyt ilmiön nimeltään Bring Your Own Device (BYOD). Bring Your Own Device tarkoittaa mahdollisuutta käyttää henkilökohtaisia mobiililaitteita työntekoon ajasta ja paikasta riippumatta. (Zahadat, Blessner, Blackburn & Olson, 2015.) Tässä tutkielmassa mobiililaitteilla tarkoitetaan työntekijöiden kannettavia tietokoneita, tabletteja, sekä matkapuhelimia. Erityisesti tutkielmassa keskitytään tabletteihin ja matkapuhelimiin.

Omien mobiililaitteiden käyttö tuottaa etuja myös organisaatioille, mutta Gaffin (2015) mukaan suurena syynä BYOD-ilmiön yleistymiseen on myös se tosiasia, etteivät monet organisaatiot kuitenkaan pystyisi estämään omien mobiililaitteiden käyttöä. Eduistaan huolimatta työntekijöiden mobiililaitteet ovat kuitenkin muodostaneet organisaatioille huomattavan tietoturvauhan. BYOD-ilmiön myötä työntekijät säilyttävät mobiililaitteissan usein myös organisaation luottamuksellista dataa, joka voi joutua vääriin käsiin monin eri tavoin. Mobiililaitteet ovat myös mahdollinen kanava erilaisille organisaatiota vastaan kohdistuville hyökkäyksille. (Zahadat ym., 2015.) Mikäli organisaatiot haluavat puolustautua mobiililaitteiden lukemattomilta tietoturvauhilta, on Gaffin (2015) mukaan organisaatioiden pakko ottaa käyttöön selvät BYOD-käytännöt ja riittävät hallintamenetelmät.

Tämän kandidaatin tutkielman tarkoituksena on selvittää, minkälaisia tietoturvauhkia BYOD aiheuttaa organisaatioille ja miten uhat voivat toteutuessaan vaikuttaa organisaation toimintaan. Lisäksi tutkielmassa esitellään erilaisia teknisiä ratkaisuja, joilla tietoturvariskejä voidaan hallita, sekä kerrotaan, minkälaisia rajoitteita hallintakeinoihin liittyy. Tutkielma pyrkiikin vastaamaan seuraaviin tutkimuskysymyksiin:

- Minkälaisia tietoturvariskejä organisaatiot kohtaavat BYOD-ympäristössä ja mitä vaikutuksia niillä toteutuessaan on organisaatiolle?
- Minkälaisilla teknisillä ratkaisuilla BYOD-ympäristön aiheuttamia tietoturvariskejä voidaan organisaatioissa hallita ja mitä rajoitteita hallintakeinoihin liittyy?

Mobiililaitteiden tarkka valvonta saattaa olla hyvin ongelmallista myös työntekijän näkökulmasta, sillä se saattaa vaarantaa esimerkiksi työntekijän yksityisyyden suojan (Zahadat ym., 2015). Tässä tutkielmassa BYOD-ilmiötä ja sen aiheuttavia tietoturvariskejä käsitellään kuitenkin organisaation näkökulmasta. Organisaatiolla viitataan tässä tutkielmassa lähinnä yrityksiin, mutta tietoturvauhat ja niiden hallintakeinot ovat oleellisia kaikissa organisaatioissa, joissa ihmisillä on mobiililaitteiden kautta pääsy organisaation dataan. Myös mobiililaitteiden käyttäjiin viitataan tässä tutkielmassa työntekijöinä. Hallintamenetelmät on tässä tutkielmassa rajattu erilaisiin teknisiin ratkaisuihin, eikä esimerkiksi työntekijöiden kouluttamista tai organisaatioiden ohjeistuksia käsitellä kattavasti. Tutkielmassa ei myöskään vertailla kaupallisia tuotteita keskenään, eikä niiden soveltumista arvioida tarkasti esimerkiksi eri käyttöjärjestelmille.

Työntekijöiden mobiililaitteiden aiheuttamia tietoturvauhkia ja niiden hallintaa on käsitelty paljon ennenkin. Useimmissa julkaisuissa keskitytään kuitenkin yleensä vain muutamiin hallintakeinoihin tai tietoturvauhkiin. Tässä tutkielmassa tarkoituksena on luoda kattava kuvaus erilaisista tietoturvauhista ja esitellä useita erilaisia teknisiä ratkaisuja uhkien hallintaan. Tässä tutkielmassa ei myöskään keskitytä ainoastaan eri hallintamenetelmien ominaisuuksiin, vaan käsitellä myös tarkemmin niiden toimintaa ja tuoda esiin niihin liittyviä rajoitteita ja ongelmia.

Lähdekirjallisuuden perusteella löydettiin useita eri tietoturvauhkia, joista tässä tutkielmassa esitellään haittaohjelmat, palvelunestohyökkäykset, sosiaalinen manipulointi, mobiililaitteiden katoaminen ja varkaus, sekä työntekijöiden huolimaton toiminta ja mobiililaitteiden huono suojaus. Näiden uhkien vaikutukset liittyivät pääasiassa organisaation järjestelmien vahingoittumiseen ja niiden toiminnan häiriöihin, sekä organisaation datan menettämiseen ulkopuoliselle taholle.

Tietoturvariskien hallintakeinoista tässä tutkielmassa esitellään mobiililaitehallinta, mobiilisovellushallinta, mobiilisisällön hallinta, yritysten mobiiliuden hallinta, pääsynhallinta tietoverkkoihin, sekä virtualisoinnin eri soveltamismuotoja. Lähdekirjallisuuden perusteella voidaan kuitenkin sanoa, että vaikka BYOD nousi Gartnerin (2012) hyperkäyrän huipulle jo vuonna 2012, eivät ainakaan tässä tutkielmassa esitellyt hallintamenetelmät ole vielä täydellisiä ratkaisuja tietoturvauhkien hallintaan. Kaikissa hallintakeinoissa on rajoitteita, eikä yksikään ratkaisu välttämättä tarjoa riittävää suojaa esimerkiksi kehittyneitä hyökkäyksiä vastaan. Aihe tuleekin todennäköisesti olemaan ajankohtainen vielä pitkään ja uskon, että etenkin uusien IOT-laitteiden (eng. Internet Of

Things) saapuminen työpaikoille tulee todennäköisesti tuottamaan vielä täysin uudenlaisia haasteita.

Tutkielma on suoritettu kirjallisuuskatsauksena ja lähdekirjallisuuden etsintään on käytetty useita tietokantoja, mukaan lukien IEEE Xplore, ScienceDirect ja Google Scholar. Lähdekirjallisuus muodostuu lähinnä vertaisarvioiduista lehtijulkaisusta, sekä tutkielman teknisen luonteen vuoksi erilaisista konferenssiseissa julkaistuista tutkimusartikkeleista. Tutkielmassa käytetään lähteenä myös muutamia suurten teknologiayritysten julkaisuja. Kaikki lähdemateriaali on haettu sähköisesti. Tutkimusprosessi alkoi lähdekirjallisuuden etsinnällä ja arvioinnilla, sekä perehtymisellä aiheen käsitteisiin ja osa-alueisiin. Näiden perusteella tutkielmasta luotiin tutkimussuunnitelma. Vaikka tutkielmassa ei tarkasti käsitelläkään erilaisia kaupallisia ratkaisuja, tutustuttiin tutkielman edetessä myös useisiin BYOD-uhkien torjuntaan tarkoitettuihin kaupallisiin tuotteisiin kokonaiskuvan hahmottamiseksi nykytilanteesta.

Tutkielman toisessa luvussa BYOD-ilmiötä käsitellään laajemmin ja kerrotaan, mitä BYOD oikeastaan käytännössä tarkoittaa, ja mikä on BYOD-ilmiön tilanne tällä hetkellä. Lisäksi luvussa kerrotaan mitä hyötyä BYOD aiheuttaa niin työntekijöille kuin myös organisaatioille ja alustetaan siihen liittyviä haasteita ja tietoturvauhkia. Kolmannessa luvussa käsitellään erilaisia tietoturvauhkia, joita organisaatiot kohtaavat BYOD-ympäristössä. Neljännessä luvussa käsitellään erilaisia teknisiä ratkaisuja, joita organisaatiot voivat hyödyntää tietoturvariskien hallintaan. Tämän jälkeen esitetään vielä yhteenveto, jossa tietoturvariskejä ja niiden hallintakeinoja arvioidaan kokonaisuutena ja esitetään taulukot tietoturvauhista ja niiden mahdollisista vaikutuksista, sekä hallintakeinoista ja niihin liittyvistä rajoitteista.

2 BYOD – BRING YOUR OWN DEVICE

Tässä luvussa avataan Bring Your Own Device -käsitettä, ja kerrotaan mitä sillä käytännössä tarkoitetaan. Tämän jälkeen kerrotaan BYOD-ilmiön nykytilanteesta ja siitä, miten omia mobiililaitteita hallitaan tällä hetkellä organisaatioissa. Lopuksi luvussa kerrotaan mitä etuja omien mobiililaitteiden käyttö työtarkoituksiin tuo organisaatoille ja työntekijöille, sekä alustetaan ilmiöön liittyviä ongelmia ja tietoturvauhkia.

2.1 Mikä on BYOD?

Bring Your Own Device -ilmiö syntyi osana informaatioteknologian kuluttajistumista. Kuluttajistumisella tarkoitetaan alun perin kuluttajamarkkinoille tarkoitetun tietotekniikan siirtymistä yrityksiin ja muihin organisaatioihin. (Vignesh & Asha, 2015.) Kuluttajistumista käytetään myös synonyyminä Bring Your Own Device -ilmiölle (Dernbecher, Beck & Weber, 2013). Bring Your Own Device on ilmiö, jossa työntekijät voivat tuoda omia mobiililaitteitaan työpaikalle ja käyttää niitä työtarkoituksiin. Työntekijät voivat esimerkiksi käyttää organisaation ohjelmistoja, sähköpostia tai tietokantoja, tai luoda, säilyttää ja hallita organisaation informaatiota mobiililaitteidensa avulla. (Bello, Murray & Armarego, 2017.) Työntekijät eivät käytä mobiililaitteitaan työtarkoituksiin ainoastaan työpaikalla, vaan myös sen ulkopuolella. Lisäksi työntekijät käyttävät samoja mobiililaitteita vapaa-ajallaan omiin henkilökohtaisiin tarkoituksiinsa. Laitteet eivät siis sisällä ainoastaan heidän omaa henkilökohtaista dataansa, vaan usein myös organisaatioiden dataa ja informaatiota. (Rivadeneira & Rodrigues, 2018.) Lisäksi työntekijöillä on pääsy organisaation dataan myös työpaikan ulkopuolelta (Olalere, Abdullah, Mahmod & Abdullah, 2015). BYOD-termillä ei kuitenkaan viitata pelkästään mobiililaitteisiin. Morrowin (2012) mukaan työntekijät tuovat työpaikalle mukanaan myös omia ohjelmistojaan ja käyttävät organisaatioiden omien palvelujen lisäksi myös muita palveluja. Monet työntekijät ha-

luavat käyttää omia mobiililaitteitaan työtehtäviinsä muun muassa siksi, että he ovat tottuneet omiin laitteisiinsa, sekä niiden käyttöjärjestelmiin ja pitävät niiden käyttöä helpompina verrattuna työnantajan tarjoamiin laitteisiin (Meske, Stieglitz, Brockmann & Ross, 2017).

BYOD ei ole ilmiönä aivan uusi ja se voidaan katsoa alkaneen jo vuonna 2003 (Leavitt, 2013). Termi BYOD esiteltiin kuitenkin vasta vuonna 2009, kun Intel huomasi työntekijöidensä halun ja tarpeen käyttää omia mobiililaitteitaan työtehtävissään (Franklin & Ismail, 2015). BYOD-ilmiö alkoi kunnolla voimistua vuonna 2011 (Leavitt, 2013). Leavittin (2013) mukaan jo vuonna 2013 BYOD ei ollut enää vain trendi, vaan sitä voitiin pitää jo uutena mallina. Palanisamyn, Normanin ja Kiahin (2020) mukaan omien mobiililaitteiden käyttämistä työnteossa voidaan pitää nykyään jo vakiokäytäntönä.

2.2 Nykyinen tila ja yleisyys organisaatioissa

Syntonic (2016) julkaisi vuonna 2016 kyselytutkimuksen, jossa selvitettiin matkapuhelinten käyttöä työntarkoituksiin eri organisaatioissa. Kyselyyn vastasi johtotason henkilöitä organisaatioista, joissa työskentelee yli 100 työntekijää. Tutkimuksen mukaan 36 % vastanneista työskenteli organisaatiossa, jossa yli puolet työntekijöistä käyttää omia matkapuhelimiaan työntekoon. 87 % vastas myös, että organisaatiot olivat jollakin tasolla riippuvaisia siitä, että työntekijät kykenevät käyttämään organisaation palveluita henkilökohtaisilla mobiililaitteillaan. 77 % vastanneista myös odotti, että matkapuhelinten käyttö työtarkoituksiin tulee lähivuosina kasvamaan. (Syntonic, 2016.)

BYOD on siis organisaatioissa jo hyvin yleinen ilmiö. Huolimatta siitä, että mobiililaitteita käytetään jo todella monissa yrityksissä, on monissa organisaatioissa kuitenkin varauduttu huonosti sen aiheuttamiin tietoturvariskeihin. Bellon, Murrayn ja Armaregon (2017) tekemässä tutkimuksessa 75 % työntekijöistä vastasi, että organisaatio, jossa he työskentelevät, ei vaadi työntekijöitä huolehtimaan mobiililaitteidensa turvallisuudesta esimerkiksi käyttämällä salasanoja ja huolehtimalla mobiililaitteiden ajantasaisista päivityksistä. kahden kolmasosan mukaan organisaatioissa mobiililaitteita ei myöskään hallita riittävästi. Työntekijöitä ei kehotettu varomaan epäluotettavia ohjelmistoja, eikä kannustettu raportoimaan kadonneesta tai varastetusta mobiililaitteesta. 42 % vastanneista ei myöskään tiennyt kehen heidän tulisi ottaa yhteyttä, mikäli heidän mobiililaitteensa saisi esimerkiksi haittaohjelmatartunnan. (Bello ym., 2017.)

2.3 Hyödyt ja haasteet

Omien mobiililaitteiden sallimisella työympäristössä on monia hyötyjä niin työntekijöille, kun myös organisaatioille. Työnantajien näkökulmasta suurimpia syitä siihen, miksi organisaatiot ovat siirtyneet BYOD-ympäristöön, on sen mahdollistamat alentuneet laite-, ohjelmisto-, ja ylläpitokustannukset. Työntekijät pitävät myös usein parempaa huolta heidän itse ostamistaan laitteista. (Ophoff & Miller, 2019.) Rosen (2013) mukaan BYOD saattaa kuitenkin myös lisätä organisaatioiden kokonaiskustannuksia, koska työnantajat joutuvat hallitsemaan monia erilaisia laitteita, käyttöjärjestelmiä, sekä käyttöjärjestelmien eri versioita. Koska työntekijät käyttävät omia laitteitaan myös puheluihin, organisaatio saattaa menettää brändi-identiteettiään. Puhelinnumerot voivat olla iso osa organisaation brändi-identiteettiä, mutta omien mobiililaitteiden myötä yritykset saattavat menettää hallinnan siihen, mistä numerosta yrityksen asioita hoidetaan. (Rose, 2013.) BYOD-ympäristön on huomattu lisäävän työntekijöiden tuottavuutta. Intelin (2011) tekemän tutkimuksen mukaan työntekijät säästävät keskimäärin noin 47 minuuttia päivässä käyttämällä omia mobiililaitteitaan työntekoon. Omien laitteiden käyttäminen vähentää lisäksi teknisen tuen tarvetta organisaatioissa (Alotaibi & Almagwashi, 2018).

Omien mobiililaitteiden salliminen lisää työntekijöiden itsenäisyyttä ja vapautta, sekä lisää heidän tyytyväisyyttään (Niehaves, Köffer, Orthbach, 2012). Dellin ja Intelin (2011) tekemän tutkimuksen mukaan kuusi kymmenestä työtekijästä nauttii työstään enemmän, jos he saavat käyttää työssään omia laitteitaan ja teknologioitaan. Työntekijöiden tyytyväisyys lisää myös heidän työnsä tuottavuutta (Saari & Judge, 2004). BYOD mahdollistaa työskentelyn myös työpaikan ulkopuolella, joka lisää työn joustavuutta, sekä mahdollistaa työnteon jatkuvuuden (Lebek, Degirmenci & Breitner, 2013). Työntekijät pitävät myös houkuttelevampina yrityksiä, jotka toimivat BYOD-ympäristössä (Weeger, Wang & Gewald, 2015). Työntekijöiden tyytyväisyyttä lisää muun muassa se, että he ovat usein tottuneempia omiin laitteisiinsa ja osaavat käyttää niitä paremmin verrattuna työnantajan tarjoamiin laitteisiin. Lisäksi työntekijät pystyvät ratkaisemaan ongelmia nopeammin heille tutuilla laitteilla. (Niehaves ym., 2012.) Työntekijöiden tyytyväisyys työhönsä paranee myös siksi, koska heidän ei tarvitse käyttää useampaa laitetta eri tarkoituksiin, vaan he voivat hoitaa samalla laitteella niin yksityiselämän asiat, kuin työnkin (Disterer & Kleiner, 2013).

Huolimatta BYOD-ilmiön aiheuttamista positiivisista vaikutuksista, aiheuttaa omien mobiililaitteiden salliminen yrityksille myös huomattavia haasteita ja ongelmia. 90 % pöytätietokoneissa esiintyvistä haavoittuvuuksista löytyvät myös mobiililaitteista käyttöjärjestelmästä riippumatta (Leavitt, 2013). BYOD-ympäristössä mobiililaitteet kohtaavat samoja uhkia, kun mobiililaitteet yleensäkin (Tse, Wang & Li, 2016). Henkilökohtaiset mobiililaitteet ovat myös usein huonosti suojattuja, eikä niissä ole tarpeellisia tietosuojapäivityksiä tai -asetuksia (Gajar, Ghosh & Rai, 2013).

Henkilökohtaisten mobiililaitteiden käyttö nimenomaa työtarkoituksiin ja liittyminen niillä organisaation verkkoon, aiheuttaa kuitenkin myös omanlaisiaan haasteita ja tietoturvauhkia. Koska mobiililaite sisältää usein niin organisaation kuin myös työntekijän dataa, tasapainon löytäminen mobiililaitteiden riittävän valvonnan ja työntekijöiden yksityisyydensuojan välillä voi olla hyvin vaikeaa. (Gajar ym., 2013.) Työntekijän mobiililaite voi aiheuttaa organisaatioille hyvin suuria tietoturvauhkia, mutta toisaalta mobiililaitteiden valvonta voi vaarantaa työntekijöiden yksityisyyden suojan (Perakovic, Husnjak & Cvitic, 2014). Liian tarkka valvonta tai toiminnan rajoittaminen saattaa myös rajoittaa hyötyjä, joita BYOD organisaatiolle aiheuttaa.

3 TIETOTURVAUHAT BYOD-YMPÄRISTÖSSÄ

Huolimatta siitä, että BYOD tuottaa organisaatioille monenlaisia hyötyjä, liittyy siihen myös huomattavia riskejä. Tietoturva on suurimpia haasteita, joita organisaatiot kohtaavat BYOD-ympäristössä. Tietoturva on ennenkin ollut huomattava ongelma eri organisaatioille, mutta BYOD aiheuttaa myös aivan uudenlaisia haasteita. BYOD mahdollistaa samojen mobiililaitteiden käytön ajasta ja paikasta riippumatta niin työssä, kuin myös vapaa-ajalla. Työntekijöiden mobiililaitteet voivat siis vaarantua missä ja milloin vain ja uhka ei koske ainoastaan työntekijöiden dataa, vaan myös organisaatioita, joissa he työskentelevät. (Leavitt, 2013.)

Tässä luvussa esitellään yleisiä tietoturvauhkia, joita organisaatiot kohtaavat BYOD-ympäristössä. Vaikka samoja tietoturvauhkia esiintyy myös organisaatioissa, joissa omia mobiililaitteita ei sallita, ovat luvussa esitellyt tietoturvariskit ovat erityisen merkityksellisiä BYOD-kontekstissa (Flores, Qazi & Jhumka, 2016). Tässä luvussa käsitellään mobiililaitteiden haittaohjelmia, palvelunestohyökkäyksiä, sekä työntekijöiden sosiaalista manipulointia ja kalasteluhyökkäyksiä. Lisäksi luvussa käsitellään mobiililaitteiden katoamista ja varkautta, sekä työntekijöiden omasta toiminnasta johtuvia tietoturvauhkia.

3.1 Haittaohjelmat

Mobiilihaittaohjelmalla (eng. mobile malware) tarkoitetaan haitallista ohjelmistoa, joka on suunniteltu tuottamaan vahinkoa käyttäjien mobiililaitteille. Useimmiten niiden tarkoitus on lamauttaa mobiililaite, jolloin hyökkääjä voi ottaa mobiililaitteen hallintaansa ja esimerkiksi varastaa laitteessa sijaitsevia käyttäjän tietoja. (Wu, Narang & Clarke, 2014.) Koska BYOD-ympäristössä työntekijöiden mobiililaitteet sisältävät usein myös organisaation luottamuksellista tietoa, saatetaan nekin menettää haittaohjelmatartunnan seurauksena. Haittaohjelmat saattavat vahingoittaa myös yritysten sovelluksia tekemällä niistä käyttökelvottomia tai muuten vaikuttamalla niiden toimintaan. (Olalere

ym., 2015.) Haittaohjelma saattaa tarttua mobiililaitteisiin esimerkiksi heidän vapaa-ajallaan ja levitä organisaation laitteisiin ja tietoverkkoihin työntekijöiden liittyessä niihin (Miller, Voas & Hurlburt, 2012). Mobiililaitteet voivat saada haittaohjelmatartunnan lukuisia kanavia pitkin kuten esimerkiksi tekstiviestien, multimediaviestien, bluetoothin tai internetin välityksellä (La Polla, Martinelli & Sgandurra, 2012). Haittaohjelmia voidaankin pitää yhtenä suurimmista uhista BYOD-ympäristössä toimiville organisaatoille (Olalere ym., 2015).

Haittaohjelmia on useita erilaisia ja ne voidaan jakaa eri kategorioihin. Yleisiä haittaohjelmatyyppejä ovat muun muassa troijalaiset, virukset, madot, vakoiluohjelmat, sekä bottiverkot (Peng, Yu & Yang, 2014).

Troijalaisella (eng. trojan horse) tarkoitetaan haitallista ohjelmaa, joka usein naamioituu luotettavaksi ohjelmaksi, kuten mobiilipeliksi, suorittaakseen haitallia toimia kohteen laitteessa (Aliyu, Danjuma, Waziri, Ado & Dai, 2014). Usein käyttäjät huijataan lataamaan troijalainen laitteeseen ja käynnistämään se, jolloin se voi esimerkiksi vahingoittaa laitetta poistamalla sieltä tiedostoja. Troijalainen voi myös varastaa dataa laitteista, tai levittää laitteisiin muita haittaohjelmia, kuten esimerkiksi viruksia. (Peng ym., 2014.) Toisin kuin esimerkiksi madot, troijalaiset eivät monista itseään ja pyri tartuttamaan itseään muihin laitteen tiedostoihin (Aliyu ym., 2014). Troijalaiset jättävät usein myös takaovia, joiden avulla hyökkääjä saa pääsyn kohteen laitteeseen ja pystyy kontrolloimaan sitä (Peng ym., 2014).

Virus on haittaohjelma, joka tunkeutuu laitteeseen käyttäjän tietämättä ja liittää itsensä johonkin tiedostoon. Virukset pystyvät usein myös monistautumaan, mutta ne vaativat siihen apua käyttäjältä tai järjestelmältä. Virukset eivät kuitenkaan ole enää niin yleisiä haittaohjelmia kuin ennen. (Alwahedi, Ali, Ishowo-Oloko, Woon & Aung, 2017.)

Madot (eng. worm) ovat hyvin samankaltaisia kuin virukset, mutta ne pystyvät monistamaan itseään täysin itsenäisesti ilman käyttäjien vaikutusta (Alwahedi ym., 2017). Madot saattavat levittää itsestään satoja tai jopa tuhansia kopioita, ja tuottaa merkittävää haittaa internetliikenteelle, verkkosivuille, sekä käyttäjien laitteille (Peng ym., 2014).

Vakoiluohjelmien (eng. spyware) tarkoituksena on vakoilla kohteiden järjestelmiä ja kerätä tietoa esimerkiksi käyttäjien sähköposteista, tekstiviesteistä, käyttäjätunnuksista tai muusta käyttäjän laitteella sijaitsevasta informaatiosta. Vakoiluohjelmat saattavat levitä mobiililaitteisiin esimerkiksi tekstiviestilinkkien tai sähköpostiliitteiden kautta. (Wu ym., 2014.)

Bottiverkoilla (eng. botnet) tarkoitetaan joukkoa laitteita, jotka ovat saanet haittaohjelmatartunnan, ja joita hyökkääjä voi hallita etäältä. Bottiverkkoon kuuluvien laitteiden käyttäjät eivät useimmiten ole tietoisia siitä, että he ovat osa verkkoa. Suurin osa bottiverkoista on kehitetty järjestäytyneelle rikollisuudelle tarkoituksenaan tienata heille rahaa. Bottiverkot voivat esimerkiksi lähettää roskapostia, suorittaa palvelunestohyökkäyksiä, tai kerätä informaatiota laittomiin tarkoituksiin. (La Polla ym., 2012.) Bottiverkot kehittyvät jatkuvasti ja ne koostuvat aina vain enemmän mobiililaitteista. Ne voivat olla myös hyvin

hankalia havaita. Bottiverkkoja voidaankin pitää erityisen suurena tietoturvauhkana BYOD-ympäristössä toimiville organisaatioille. (Eslahi ym., 2014.)

3.2 Palvelunestohyökkäykset

Palvelunestohyökkäyksillä (DoS) (eng. Denial-of-Service-attack) tarkoitetaan hyökkäyksiä, joiden tarkoitus on ylikuormittaa tai vahingoittaa verkkopalveluista vastaavaa kohdejärjestelmää ja täten estää oikeutettuja käyttäjiä käyttämästä palvelua. Palvelunestohyökkäyksiä voidaan tehdä useilla eri tavoilla. Yksi keino on haavoittuvuushyökkäys (eng. vulnerability attack), jonka tarkoitus on etsiä haavoittuvuuksia kohdejärjestelmistä ja niiden avulla kaataa järjestelmät tai hankaloittaa niiden toimintaa. Toinen keino on tulvahyökkäys (eng. flooding attack), jossa hyökkääjä lähettää suuren määrän viestejä kohdejärjestelmään ja aiheuttaa näin verkon ruuhkautumisen. Tämä kuluttaa vastaanottajan resursseja niin paljon, että järjestelmä ei enää toimi oikealla tavalla, vaan voi jumiutua tai kaatua. (Farina, Cambiaso, Papaleo & Aiello, 2015.)

Hajautettu palvelunestonhyökkäys (DDoS) (eng. Distributed-Denial-of-Service-attack) on palvelunestohyökkäystyyppi, jossa hyökkääjä käyttää yhtä tai useampaa zombiksi kutsuttua haittaohjelmatartunnan saanutta laitetta hyökkäyksen toteuttamiseen. Laitteet voivat esimerkiksi olla osa bottiverkkoa. Hajautettu palvelunestohyökkäys on vaarallisempi kuin yhdellä laitteella toteutettu palvelunestohyökkäys ja se voi aiheuttaa hyvin vakavia ongelmia kohdejärjestelmissä ja tietoverkoissa. Hajautettuja palvelunestohyökkäyksiä voidaan toteuttaa käyttämällä hyväksi monenlaisia laitteita, mobiililaitteet mukaan lukien. Hajautetun palvelunestohyökkäyksen havaitseminen voi olla myös hyvin vaikeaa, koska verkkoliikennettä tulee useasta lähteestä ja hyökkääjät yleensä vain antavat ohjeita muille laitteille suorittamatta itse varsinaista hyökkäystä. (Yuvaraj, Sivaram, Ayoobkhan & Negeswari, 2019.) Jos hyökkääjä esimerkiksi yrittää toteuttaa tulvahyökkäyksen yhdellä laitteella kohdetta heikommalla verkkoyhteydellä, ei hyökkäys onnistu. Hajautetussa palvelunestohyökkäyksessä hyökkääjä voi kuitenkin käyttää apunaan useita laitteita ja mahdollistaa tällä tavalla tulvahyökkäyksen onnistuminen. (Farina ym., 2015.) Etenkin hajautettujen palvelunestohyökkäyksien on havaittu olevan suuri uhka BYOD-ympäristössä toimiville organisaatioille ja ne voivat muun muassa estää työntekijöitä käyttämästä mobiililaitteitaan organisaation tietoverkoissa tai altistaa organisaation toisille uhille tai hyökkäyksille, jotka voivat vaarantaa organisaation luottamuksellisen datan. Lisäksi mikäli tietoverkkoihin liityttäessä ei käytetä tarpeeksi vahvaa tunnistautumista, saattaa hyökkääjä esittää olevansa tietoverkon oikeutettu käyttäjä suorittaessaan hyökkäystään. (Olalere ym., 2015.)

3.3 Sosiaalinen manipulointi ja tietojen kalastelu

Sosiaalisen manipuloinnin (eng. social engineering) tarkoituksena on eri keinoja käyttämällä saada hyökkäyksen kohteet vaarantamaan tietojärjestelmiä. Teknisten hyökkäysten sijaan hyökkääjä voi esimerkiksi pyrkiä manipuloimaan käyttäjiä antamaan luottamuksellista tietoa, tai suorittamaan itse haitallisia hyökkäyksiä. Sosiaalisen manipuloinnin keinoja on erilaisia. Hyökkääjä voi esimerkiksi suostutella uhrin antamaan tietojaan esittämällä jonkinlaista auktoriteettia. Hyökkääjä pyrkii usein myös selvittämään etukäteen tietoja uhristaan tai kehittämään hänen kanssaan sosiaalisia suhteita. (Krombholz, Hobel, Huber & Weippl, 2015.) BYOD-ympäristössä hyökkääjä voi esimerkiksi houkutella työntekijän antamaan tietoja organisaatiostaan tai muilla keinoilla saada työntekijää hyödyntämällä haltuunsa organisaation dataa (Flores ym., 2016).

Sosiaalista manipulointia voidaan suorittaa myös käänteisesti (eng. reverse social engineering). Tämän tarkoituksena on saada uhri ottamaan itse yhteyttä hyökkääjään. Hyökkääjä esimerkiksi saattaa esittää pysyvänsä korjaamaan jonkun uhrin ongelman. Ongelma on kuitenkin mahdollisesti aiheutettu hyökkääjän toimesta, ja hän on voinut esimerkiksi itse kytkeä uhrin ulos organisaation verkosta. (Krombholz ym., 2015.)

Kalasteluhyökkäykset (eng. phishing) ovat yksi yleinen sosiaalisen manipuloinnin muoto. Hyökkääjä pyrkii huijaamaan käyttäjiä esittäytymällä jonakin luotettavana toimijana. Niin kuin monissa muissakin sosiaalisen manipuloinnin muodoissa, hyökkääjän tarkoituksena on useimmiten saada haltuunsa uhrien henkilökohtaisia tietoja, kuten esimerkiksi salasanoja, käyttäjätunnuksia, sekä pankkitunnuksia. Mobiiliympäristössä kalastelu suoritetaan usein lähettämällä uhreille tekstiviestejä tai sähköposteja, jotka sisältävät linkkejä kalastelusivuille. Näillä sivuilla uhria pyydetään usein antamaan erilaisia tietoja, kuten kirjautumaan sisään omalla salasanallaan. (Shahriar, Klintic & Clincy, 2015.) Kalasteluhyökkäyksiä voidaan kuitenkin suorittaa useita muitakin kanavia pitkin. Hyökkääjä voi esimerkiksi levittää linkkejä kalastelusivuille sosiaalisessa mediassa tai muilla internetsivuilla tai yrittää saada haltuunsa uhrien tietoja pilvipalveluihin sijoitettujen tiedostojen ja ohjelmien avulla. (Krombholz ym., 2015.) Koska työntekijät käyttävät mobiililaitteitaan BYOD-ympäristössä niin työkäyttöön, kuin myös omaan henkilökohtaiseen käyttöönsä, saattaa esimerkiksi linkkien painaminen sosiaalisessa mediassa levittää haittaohjelmia organisaation verkkohiin. Työntekijät saattavat myös syöttää kalastelusivustoille tietoja, joita hyökkääjä voi käyttää organisaation tietojen varastamiseksi. (Flores ym., 2016.)

Mobiililaitteiden käyttäjät ovat suuremmassa vaarassa joutua tietojen kalastelun kohteeksi verrattuna pöytätietokoneiden käyttäjiin. Mobiililaitteiden pienemmän koon vuoksi käyttäjän voi olla hankala erottaa turvallista sivustoa tai sovellusta hyökkääjän luomasta kalastelusivusta tai sovelluksesta. Laillisissa sivustoissa ja sovelluksissa on usein hyvin yksinkertaiset käyttöliittymät, joita hyökkääjän on helppo jäljitellä. Myöskään web-osoitteita ei välttämättä näytetä kokonaan mobiililaitteiden selaimissa. On myös hyvin yleistä, että täysin lailli-

set mobiilisovellukset vaativat käyttäjää syöttämään palveluun oman salasanansa. Tämä voi hankaloittaa täysin turvallisten sovellusten erottamista hyökkääjien tekemistä vaarallisista sovelluksista ja sivustoista. (Shahriar ym., 2015.)

3.4 Mobiililaitteiden katoaminen ja varkaus

Yli sata mobiililaitetta joutuu kadoksiin joka minuutti, usein varkauden seurauksena (Prowse, 2015). Tu, Yuan ja Archer (2014) tekivät tutkimuksen, jossa 40 % vastanneista käytti mobiililaitteitaan myös työpaikallaan ja heistä 26 % oli myös hävittänyt laitteensa ainakin kerran. Verrattuna esimerkiksi pöytätietokoneisiin, mobiililaitteet katoavat hyvin helposti. Mobiililaitteet ovat suurempiin laitteisiin verraten myös varsin helppo varastaa. Koska BYOD mahdollistaa samojen mobiililaitteiden käytön niin vapaa-ajalla kuin työssäkin, voi laitteen katoaminen olla erittäin suuri riski organisaatioille (Morrow, 2012). Mobiililaitteet ovat usein myös huonosti suojattuja ja mikäli mobiililaitteita ei kontrolloida mitenkään, tiedot löytyvät mobiililaitteista täysin salaamattomina, eikä mobiililaitetta ole mahdollisuutta esimerkiksi etäpyyhkiä, riski organisaation datan joutumisesta vääriin käsiin on erittäin suuri (Prowse, 2015).

3.5 Mobiililaitteiden heikko suojaus ja huolimaton käyttö

Huolimatta siitä, että BYOD-ympäristössä toimiva organisaatio voi kohdata useita ulkopuolisia uhkia, saattavat työntekijät myös vaarantaa itse organisaation turvallisuuden, joko tahallisesti, tai tahattomasti (Flores ym., 2016). Yksi yleinen tietoturvariski on mobiililaitteiden roottaus (eng. root tai IOS-ympäristössä jailbreak). Roottaus tarkoittaa mobiililaitteiden ohjelmallista ”avaamista”, ja se usein poistaa laitteeseen alun perin asetettuja tietoturvarajoituksia, ja antaa muun muassa mahdollisuuden asentaa laitteeseen kolmansien osapuolien ohjelmistoja. Tämä kasvattaa riskiä esimerkiksi haittaohjelmatartunnoille. (Harris, Patten & Regan, 2013.)

Toinen tietoturvariski on työntekijöiden mobiililaitteiden heikko suojaus. Tutkimukset osoittavat, että Yhdysvalloissa suuri osa ihmisistä ei käytä yksinkertaisiakaan suojaustoimintojaan mobiililaitteissaan, kuten esimerkiksi salasanoja. 14 % ei koskaan päivitä mobiililaitteen käyttöjärjestelmää ja 10 % ei päivitä mobiililaitteissaan olevia sovelluksia. (Belanger & Crossler, 2018.)

Työntekijät ovat usein myös huolimattomia mobiililaitteiden sisältävän datan suhteen. Bellon, Murrayn ja Armaregon (2017) tekemän tutkimuksen mukaan 14 % BYOD-ympäristössä toimivista työntekijöistä jakoi salasanojaan työkaveriensa, ystäviensä ja perheensä kanssa ja 11 % vastanneista sanoi sen olevan riippuvainen tilanteesta. Lisäksi 53 % vastanneista tallensi säännöllisesti laitteensa tiedot ulkoiselle kovalevylle tai julkiseen pilveen. (Bello ym., 2017.)

4 TIETOTURVARISKIEN HALLINTA

Tässä luvussa esitellään tapoja, joilla organisaatiot voivat hallita tietoturvauhkia BYOD-ympäristössä, sekä kerrotaan niiden toiminnasta ja rajoitteista. Organisaatiot voivat ehkäistä mobiililaitteiden aiheuttamia tietoturvauhkia muun muassa työntekijöiden koulutuksella, mutta tässä luvussa esitellään erilaisia teknisiä ratkaisuja tietoturvauhkien hallintaan. Luvussa käsitellään ensin erilaisia mobiililaitteiden hallintaan tarkoitettuja järjestelmiä, jotka ovat mobiililaitehallintajärjestelmät, mobiilisovellushallintajärjestelmät ja mobiilisisällön hallintajärjestelmät. Tämän jälkeen käsitellään myös näiden järjestelmien yhdistelmäratkaisuja, eli yritysten mobiiliuden hallintaa. BYOD-riskien hallintaan tarkoitettujen tietojärjestelmien lisäksi tässä luvussa käsitellään myös tietoverkkojen pääsynhallintaa, sekä virtualisoinnin eri hyödyntämiskeinoja tietoturvariskien hallinnassa. Luvussa käsitellään eri ratkaisujen toimintaa yleisellä tasolla, sekä esitellään niihin yleisesti kuuluvia ominaisuuksia ja rajoitteita. Kaupallisia ratkaisuja ei kuitenkaan vertailla keskenään, eikä niiden soveltumista erilaisille käyttöjärjestelmille arvioida tarkasti.

4.1 Mobiililaitehallinta

Mobiililaitehallinnalla (MDM) (eng. Mobile Device Management) tarkoitetaan järjestelmiä, joiden avulla voidaan muun muassa etäältä seurata mobiililaitteita, sekä kontrolloida niiden ominaisuuksia ja käyttöä. Mobiililaitehallinnan avulla organisaatiot voivat ohjata työntekijöiden mobiililaitteiden turvallisuutta, seurata turvallisuuskäytäntöjen noudattamista, sekä hallita MDM-järjestelmään kytkettyjen laitteiden käyttöoikeuksia. (Garba, Armarego, Murray & Kenworthy, 2015.) MDM-järjestelmiä on erilaisia, mutta niistä löytyy useimmiten ainakin seuraavia ominaisuuksia:

- **Profiilien hallinta.** MDM-järjestelmien avulla organisaatiot pystyvät asettamaan työntekijöiden mobiililaitteiden turvallisuusasetuk-

sia ja rajoituksia, sekä mukauttamaan laitteiden ominaisuuksia organisaation vaatimusten mukaisiksi.

- **Mobiililaitteiden seuranta ja jäljitys.** Mikäli työntekijän mobiililaite häviää, MDM-järjestelmät pystyvät ilmoittamaan laitteen olinpaikan. (Gajar ym., 2013.)

- **Käyttöoikeuksien hallinta.** MDM-järjestelmät pystyvät valvomaan, kellä on pääsy yrityksen verkkoihin. Työntekijät eivät myöskään pysty liittymään epäluotettaviin verkkoihin ollessaan MDM-järjestelmän valvonnassa.

- **Mobiililaitteiden etälukitus ja -pyyhintä.** Mikäli mobiililaite katoaa tai se varastetaan, MDM-järjestelmät pystyvät pyyhkimään laitteessa olevan datan tai lukitsemaan sen tietovuodon ehkäisemiseksi.

- **Haittaohjelmien havaitseminen.** Useimmat mobiililaitteiden hallintajärjestelmät kykenevät havaitsemaan haittaohjelmia ja ilmoittamaan niistä reaaliajassa. (Tse ym., 2016.)

MDM-järjestelmissä on usein myös muita ominaisuuksia, kuten mahdollisuus salata mobiililaitteissa olevaa dataa, ladata sovelluksia työntekijöiden mobiililaitteisiin ja poistaa niitä, sekä hallita muun muassa mobiililaitteiden kameroita, mikrofonia, WIFI:ä sekä bluetoothia (Rhee, Won, Jang, Chae & Park, 2013). Esimerkkejä mobiililaitteiden hallintajärjestelmistä ovat muun muassa Google device manager, Apple profile manager, sekä Microsoft exchance ActiveSync (Alotaibi & Almagwashi, 2018).

MDM-järjestelmät koostuvat tavallisesti neljästä eri komponentista:

- **MDM-agentti (MDM agent).** MDM agentilla tarkoitetaan BYOD laitteeseen asennettavaa ohjelmistoa, joka kerää tietoa käyttäjän laitteesta ja lähettää ne MDM palvelimelle. Lisäksi agentti suorittaa MDM-palvelimen lähettämät käskyt mobiililaitteessa. (Kim & Jin, 2015.)

- **MDM-palvelin (MDM server).** MDM palvelin hallitsee järjestelmään rekisteröityjen laitteiden ja käyttäjien dataa, sekä vastaa mobiililaite hallinnan käytänteistä ja ohjelmistosta.

- **MDM-hallintakonsoli (MDM console).** Hallintakonsolilla tarkoitetaan ohjelmistoa, jonka avulla järjestelmän ylläpitäjä pääsee kirjautumaan MDM palvelimelle ja hallinnoimaan mobiililaitehallinta -järjestelmää. (Rhee ym., 2013.)

- **MDM-yhdyskäytäväpalvelin (MDM gateway server).** Yhdyskäytäväpalvelin sijaitsee demilitarisoidulla alueella (eng. demilititarized zone). Demilitarisoidulla alueella tarkoitetaan tietoverkkoa, joka sijoitetaan organisaation sisäisen suojatun verkon ja langattoman verkon väliin. Demilitarisoidun alueen tarkoituksena on luoda lisäsuojaa organisaation tietoverkoille. (Rababah, Zhou & Bader, 2018.) Yhdyskäytäväpalvelimen tehtävänä on hallita verkkoliikennettä BYOD-laitteiden ja organisaation verkon välillä. Palvelin muun muassa todentaa organisaation verkkoon yhdistävät mobiililaitteet, sekä mahdollistaa todennettujen laitteiden nopean uudelleenliittymisen. (Tatte & Bamnote, 2013.)

Seuraavat viisi vaihetta kuvaavat tavanomaisen MDM-järjestelmän toimintaa:

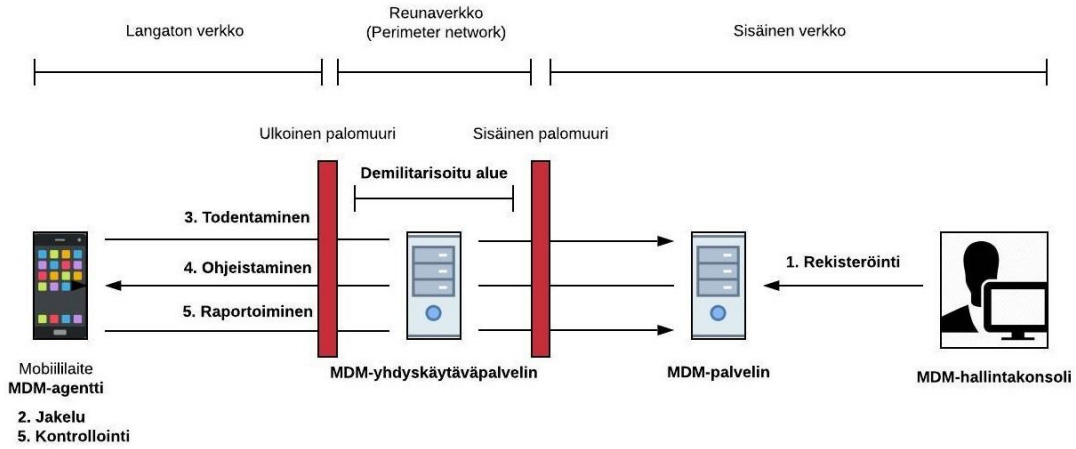
1. **Rekisteröinti.** Mobiililaitteiden ja käyttäjien tiedot rekisteröidään MDM-järjestelmään, sekä määritellään käytännöt ja asetukset, joita mobiililaitteiden tulee noudattaa.

2. **Jakelu.** MDM agentti asennetaan mobiililaitteisiin. Agentti voidaan jakaa sovelluskaupan tai organisaation kautta.

3. **Todentaminen.** Kun agentti on ladattu laitteeseen ja se käynnistetään, ohjelmisto lähettää laitteen tietoja, kuten IP-osoitteen, IMEI-koodin, tai puhelinnumeron MDM palvelimelle. Tietojen avulla MDM-palvelin voi tarkastaa, vastaavatko tiedot järjestelmään aikaisemmin rekisteröityjä tietoja.

4. **Ohjeistaminen.** MDM-palvelin lähettää laitteisiin asennetuille ohjelmistoille ohjeistuksen ja käytänteet, joita laitteiden tulee noudattaa. MDM palvelin voi lähettää agentille myös käskyjä, kuten ”poista ohjelmisto”, jolloin agentti poistaa käsketyn ohjelman mobiililaitteesta.

5. **Kontrollointi ja raportoiminen.** Mobiililaitteessa sijaitseva agentti kontrolloi laitetta ohjeistusten ja komentojen mukaan, sekä raportoi niistä MDM-palvelimelle. (Rhee ym., 2013.) (KUVIO 1)



KUVIO 1 yleistetty MDM-järjestelmän arkkitehtuuri ja toiminta (Rhee ym., 2013, Tse ym., 2016 mukaan)

MDM-järjestelmissä on monipuolisista ominaisuuksistaan huolimatta myös rajoitteita. Työntekijät pystyvät poistamaan MDM-agentin omasta mobiililaitteestaan, jolloin myös laitteisiin asetetut suojausprofiilit häviävät. Ongelmana on myös se, että BYOD-ympäristössä työntekijät voivat käyttää keskenään hyvin erilaisia laitteita. MDM-järjestelmät eivät tue kaikkia mahdollisia käyttöjärjestelmiä tai laitteita ja liitettävien laitteiden lukumäärä on rajattu. Koska työntekijät säilyttävät mobiililaitteissaan niin omaa, kun organisaationkin dataa, MDM-järjestelmät saattavat sekoittaa ne keskenään. Ongelmana voidaan pitää myös sitä, että hyödyllisten MDM ominaisuuksien käyttö edellyttää kolmansien osapuolien sovellusten lataamista mobiililaitteisiin (MDM-agentti). (Alotaibi & Almagwashi, 2018.) MDM-järjestelmien avulla ei myöskään voida kaikista kontrollointiominaisuuksista huolimatta täysin hallita käyttäjän mobiililaitetta esimerkiksi vianmääritystä varten (Garba ym., 2015). MDM-järjestelmissä on myös ominaisuuksia, joiden vuoksi työntekijöiden oma yksityinen data saattaa vaarantua. Esimerkiksi mikäli organisaatio haluaa pyyhkiä tietoja työntekijän mobiililaitteesta, saattavat myös työntekijän omat tiedot hävitä. (Dhingra, 2015.) MDM-järjestelmien avulla organisaatio saattaa pyyhkiä työntekijän tiedot myös silloin kun laite ei ole hävinnyt, esimerkiksi työntekijän vaihtaessa työpaikkaansa (Gaff, 2015).

4.2 Mobiilisovellushallinta

Mobiilisovellushallinta (MAM) (Mobile Application Management) muistuttaa paljon mobiililaitehallintaa, mutta sillä pyritään valvomaan ja kontrolloimaan tiettyjä organisaation määrittämiä ohjelmia koko mobiililaitteen sijaan. Mobiilisovellushallinnannan avulla voidaan esimerkiksi seurata ja kontrolloida organisaation sähköpostisovellusta tai muita organisaation ohjelmistoja. (Scarfo, 2012.) MAM-järjestelmillä voi kuitenkin hallita ainoastaan sellaisia ohjelmistoja, jotka on suunniteltu toimimaan organisaation käytössä olevan MAM-

järjestelmän kanssa. MAM-järjestelmistä löytyy usein seuraavanlaisia ominaisuuksia:

- **Ohjelmistojen jakelu.** Organisaatiot voivat MAM-järjestelmien avulla ladata ohjelmistoja työntekijöiden mobiililaitteisiin ilman, että ne pitäisi jakaa esimerkiksi sovelluskaupan kautta.
- **Ohjelmien lataaminen.** MAM-järjestelmien avulla voidaan estää tiettyjen ohjelmien lataaminen, sekä muistuttaa työntekijöitä tarvittavien sovellusten asentamisesta. Organisaatio voi esimerkiksi etukäteen määrittää ohjelmat, joita työntekijät eivät saa ladata mobiililaitteisiinsa. Mikäli työntekijä lataa kielletyn sovelluksen, MAM-järjestelmä lähettää siitä ilmoituksen.
- **Sovellusluettelon luominen.** Tämän ominaisuuden avulla organisaatiot voivat luoda luettelon sovelluksista helpottamaan organisaation sovellusten ja työntekijöiden omien sovellusten hallintaa. Sovellusluettelon avulla eri työntekijöille voidaan myös ottaa käyttöön eri ohjelmia.
- **Sovellusten raportointi.** MAM-järjestelmät pystyvät keräämään ohjelmien käytöstä tietoa, joka auttaa niiden valvonnassa ja hallinnassa. (Tse ym., 2016.)

Lisäksi MAM-järjestelmissä on usein mahdollisuus lukita, pyyhkiä, varmuuskopioida, sekä päivittää sen hallinnassa olevia sovelluksia (Rivadaneira & Rodrigues, 2018).

MAM-järjestelmien avulla organisaatiot voivat valvoa vain organisaation sovelluksia, mutta kaikki muu jää käyttäjän vastuulle. Mikäli työtekijä yrittää avata MAM-järjestelmän hallinnassa olevan sovelluksen, voidaan käyttäjältä vaatia esimerkiksi salasanaa, mutta valvonnan ulkopuolella oleviin sovelluksiin salasanaa ei kuitenkaan voida asettaa. Toisin sanoen MAM-järjestelmät eivät näe mitään, mikä tapahtuu muualla kuin sen valvonnassa olevissa sovelluksissa. (Scarfo, 2012.)

4.3 Mobiilisisällön hallinta

Mobiilisisällön hallinnan (MCM) (Mobile Content Management) tarkoituksena on valvomalla ja kontrolloimalla varmistaa turvallinen pääsy organisaation dataan ja varmistaa turvallinen tiedonsiirto mobiililaitteissa (Pierer, 2016, s. 50). MCM-järjestelmillä pyritään siihen, että käyttäjät voivat turvallisesti käyttää, tallentaa, päivittää ja jakaa organisaation dataa ja muuta sisältöä heidän sijainnistaan riippumatta. MCM-järjestelmät salaavat organisaation datan mobiililaitteissa ja pyrkivät estämään organisaation datan ja työntekijän henkilökohtaisen datan sekoittumisen. MCM-järjestelmät sallivat pääsyn organisaation tietoihin

vain suojattuja kanavia pitkin eli yleensä MCM-palvelujen kautta. (Oluwatimi, Midi & Bertimo, 2017.) MCM-järjestelmien avulla organisaatiot pystyvät hallinnoimaan organisaation dataa ja sen käyttöä ja jos esimerkiksi mobiililaite häviää, voidaan sensitiivinen sisältö pyyhkiä pois ilman, että koko mobiililaitteen tiedot vaarantuvat (Tse ym., 2016). MCM-järjestelmät suojaavat tietoa myös silloin kuin sitä siirretään mobiililaitteeseen tai sieltä pois (Romer, 2014). MCM-järjestelmistä ja niihin liittyvistä palveluista voi löytyä esimerkiksi seuraavia ominaisuuksia:

- **Pääsynhallinta organisaation tiedostoihin.** MCM-ratkaisujen avulla eri käyttäjille voidaan antaa erilaisia pääsyoikeuksia organisaation tietoihin ja niiden käyttöä voidaan rajoittaa estämällä esimerkiksi tiedostojen lataaminen tai muokkaaminen tietyiltä käyttäjiltä.
- **Turvallinen tietovarasto.** MCM-palveluntarjoajat tarjoavat yrityksille suojattuja tietovarastoja organisaation tietojen turvalliseen säilyttämiseen esimerkiksi julkisessa tai yksityisessä pilvessä, tai paikallisesti. MCM-palveluntarjoajat ovat myös vastuussa tietovarastojen turvallisuudesta. (Tse ym., 2016.)
- **Tietojen synkronointi ja jakaminen.** MCM-palvelujen tarjoamien pilvitietovarastojen käyttö mahdollistaa usein tietojen helpon jakamisen ja synkronoinnin mobiililaitteiden välillä (Oluwatimi ym., 2017). MCM-järjestelmät tarjoavat usein myös mahdollisuuden liittää järjestelmään muita palveluita, kuten Microsoft Sharepointin ja Google Driven, ja mahdollistaa tietojen turvallisen käsittelyn myös näissä palveluissa
- **Suojatut säiliöt datalle.** MCM-järjestelmien avulla dataa pystytään varastoimaan suojattuihin säiliöihin, joita voidaan käyttää datan, tiedostojen ja muun sisällön suojaamiseen mobiililaitteissa. (Romer, 2014.)
- **Reaaliaikainen analysointi ja raportointi.** MCM-järjestelmien avulla organisaatio pystyy seuraamaan esimerkiksi sitä, kuinka paljon jotain sisältöä, kuten dokumenttia, on tarkasteltu. Lisäksi MCM-järjestelmät analysoivat käyttäjien käyttäytymistä. (Tse ym., 2016.)

MCM-järjestelmissä ja niihin liittyvissä palveluissa on kuitenkin rajoitteita. Huolimatta siitä, että MCM-palveluihin on usein mahdollista liittää myös muita palveluja, on organisaation datan käsittely ja hallinta mahdollista vain tietyissä ennalta määritellyissä sovelluksissa ja palveluissa (Eslahi ym., 2014).

4.4 Yritysten mobiiliuden hallinta

Yritysten mobiiliuden hallinta (EMM) (eng. Enterprise Mobility Management) tarkoittaa kokonaisvaltaista ratkaisua, joka yleensä yhdistää ominaisuuksia ainakin mobiililaitehallinnasta, mobiilisovellushallinnasta, sekä mobiilisisällön hallinnasta (Knackmuß & Creuzburg, 2015). EMM-ratkaisut pyrkivät siis hallitsemaan niin laitteita ja ohjelmistoja, kuin myös dataa. Yritykset ovat huomanneet, etteivät MDM-, MAM-, ja MCM-järjestelmät tarjoa erikseen riittävää suojaa ja kustannukset nousevat erikseen hankittuina korkeiksi. Tällä hetkellä EMM-ratkaisut ovat yleisiä ja markkinoilla on useita toimijoita. (Tse ym., 2016.) EMM-ratkaisuissa on usein myös monia muita ominaisuuksia, kuten esimerkiksi sähköpostien hallintaa (eng. Mobile Email Management). Ominaisuudet vaihtelevat kuitenkin paljon eri palveluntarjoajien kesken (Oluwatimi ym., 2017). Esimerkiksi Vmware ja IBM tarjoavat EMM-ratkaisuja (Tse ym., 2016).

EMM-ratkaisut eivät kuitenkaan ole täydellisiä ja useat MDM-, MAM-, ja MCM-järjestelmien rajoitteista ja haasteista esiintyvät myös EMM-ratkaisuissa. EMM-ratkaisut eivät esimerkiksi välttämättä tue kaikkia käyttöjärjestelmiä, joita työntekijät haluaisivat käyttää työntekoon. Työntekijät saattavat myös olla tyytymättömiä kokonaisvaltaiseen BYOD-ratkaisuun. (Alotaibi & Almagwashi, 2018.) Mobiililaitteiden, -sovellusten ja -datan hallinta ei myöskään välttämättä riitä suojaamaan organisaatioita kehittyneitä hyökkäyksiä, kuten bottiverkkoja, vastaan ja uusia kehittyneitä tietoturvauhkia ilmenee jatkuvasti lisää (Eslahi ym., 2014).

4.5 Pääsynhallinta tietoverkkoihin

Pääsynhallinnalla tietoverkkoihin (NAC) (Network Access Control) tarkoitetaan verkkoratkaisua, jonka tarkoituksena on varmistaa noudattaako yhdistävä laite ennalta määriteltyjä suojauskäytäntöjä, ennen kuin se saa luvan liittyä tietoverkkoon (Lakbabi, 2015). Alun perin NAC-teknologioiden tarkoituksena oli estää tietokoneita levittämästä haitallista ohjelmakoodia organisaation tietoverkkoihin. NAC-teknologioissa on nykyään kuitenkin myös muita ominaisuuksia, jotka soveltuvat mobiililaitteiden hallintaan organisaatioissa. (Koh, Oh & Im, 2014.)

BYOD-ympäristössä työntekijät voivat käyttää useita erilaisia laitteita ja käyttöjärjestelmiä. NAC mahdollistaa kontrollin monenlaisten laitteiden turvalliseen ja hallittuun yhdistämiseen organisaation verkkoon ja sen avulla organisaation kytkimiin ja reitittimiin vodaan määrittää turvallisuusvaatimukset, jotka laitteiden tulee verkkoon liittyäkseen täyttää. (Garba ym., 2015.) Tällaisia vaatimuksia voivat olla muun muassa laitteen ajantasaiset tietoturvapäivityksen, palomuurit, sekä tarvittavat virustorjuntaohjelmistot (Musa, Muhammed & Ayesh, 2019). NAC-teknologiat mahdollistavat myös erilaisten käyttöoikeuksien määrittämisen erilaisille laitteille. Toisin sanoen erilaisille laitteille ja käyt-

täjille voidaan määrittää erilaiset vaatimukset verkkoon liittymiseksi, jakaa heidät eri ryhmiin ja antaa erilaiset oikeudet verkon käyttämiseen. NAC-teknologioiden avulla voidaan käyttää myös virtuaalilähiverkkoja (Virtual Local Area Network), joiden avulla mobiililaitteita voidaan jakaa segmentteihin verkkoliikenteen vähentämiseksi. (Garba ym., 2015.) Virtuaalilähiverkolla tarkoitetaan ryhmää käyttäjiä ja laitteita, jotka on loogisesti ryhmitelty esimerkiksi käyttäjien toiminnan tai osaston mukaan, riippumatta heidän fyysisestä sijainnistaan lähiverkossa (Hameed & Mian, 2012). NAC-teknologioita voidaan käyttää niin langattomassa, kuin langallisessakin ympäristössä (Garba ym., 2015).

NAC-teknologioissa on kuitenkin myös rajoitteita, eikä NAC ole yksinään riittävä suoja tietoturvauhkia vastaan BYOD-ympäristössä (Koh ym., 2014). Koska NAC-teknologioiden pääasiallinen tarkoitus on kontrolloida laitteiden liittymistä tietoverkkoihin, se ei pysty havaitsemaan käyttäjien poikkeavaa toimintaa verkkoon liittymisen jälkeen. Työntekijät, joilla on oikeus käyttää tietoverkkoa, voivat päästä verkkoon normaalin todennusprosessin kautta ja esimerkiksi ladata ja levittää organisaation dataa hyökkääjän suostuttelun seurauksena tai oman edun tavoittelemiseksi. NAC-teknologiat eivät myöskään pysty kontrolloimaan verkkoon liitettyjä laitteita. (Kim & Kim, 2015.) NAC-teknologioita voidaan kuitenkin käyttää myös yhdessä esimerkiksi MDM-järjestelmien kanssa (Concepcion, Chua, Siy & Ballon, 2015). NAC-teknologoissa on myös muita heikkouksia. Esimerkiksi multimediasisällön hallinta saattaa johtaa verkon ylikuormittumiseen. Verkon käyttöoikeuksien asettaminen eri laitteille voi myös olla ongelmallista, varsinkin jos käyttäjällä on verkossa useita eri laitteita. Virtuaalilähiverkkoja käytettäessä on myös mahdollista, että haittaohjelman sisältävä laite levittää sen kaikkiin muihin samassa verkossa oleviin laitteisiin. Lisäksi virtuaalisia erillisverkkoja (Virtual Private Network) käyttävät laitteet, saattavat vaarantaa organisaation tietoverkon. (Garba ym., 2015.) Virtuaalisella erillisverkolla tarkoitetaan suojattua julkisen infrastruktuurin päälle rakennettua verkkoa, jossa pääsyä valvotaan ja yhteydet sallitaan vain määritellyille henkilöille (Liotta, Tyrode-Goilo & Oredope, 2007).

4.6 Virtualisointi

Virtualisoinnilla (eng. virtualization) tarkoitetaan menetelmiä, joiden avulla voidaan simuloida laitteistoja ja ohjelmistoja (NIST, 2011). Virtualisointia voidaan toteuttaa eri tasoilla eli toisin sanoen on mahdollista virtualisoida kokonainen tietokone tai vain esimerkiksi yksittäinen ohjelma, muisti tai prosessori. (Horalek, Matyska & Sobeslav, 2013). Myös palvelimet voidaan virtualisoida, jolloin yhdellä fyysisellä palvelimella voidaan ajaa useita virtuaalisia palvelimia. Tätä kutsutaan palvelinvirtualisoinniksi (eng. server virtualization). (Jain & Choudhary, 2016.)

Yksi keino suojautua tietoturvauhilta BYOD-ympäristössä on virtuaalisen työasemaympäristön hyödyntäminen (VDI) (eng. Virtual Desktop Infrastructure). Mobiiliympäristössä VDI-ympäristöllä tarkoitetaan mahdollisuutta käyttää

virtuaalityöpöytiä erilaisten mobiililaitteiden kautta. Tämä voidaan toteuttaa joko mobiililaitteeseen asennetun ohjelmiston avulla, tai internetin välityksellä käyttämällä HTLM 5 teknologioita tukevia verkkoselaimia. Käyttötavasta riippumatta käyttäjät näkevät mobiililaitteissaan ainoastaan kuvaa simuloitavasta työpöydästä eli kaikki data ja ohjelmat sijaitsevan organisaation järjestelmissä, eivätkä mobiililaitteissa. (Perakovic ym., 2014.)

Perakovicin ym. (2014) mukaan mobiiliympäristössä VDI-ympäristön käytössä on kuitenkin useita ongelmia. Koska esimerkiksi älypuhelimissa ja tableteissa ei ole tietokoneissa käytettäviä laitteita kuten näppäimistöä ja hiirtä, voi joidenkin sovellusten käyttö olla mahdotonta. Virtuaalisen työpöydän käyttö voi olla vaikeaa myös mobiililaitteiden mahdollisen pienen koon vuoksi. Esimerkiksi alasvetovalikot saattavat jäädä tietyissä sovelluksissa kuvaruudun ulkopuolelle. (Perakovic ym., 2014.)

Toinen virtualisointikeino on laitteistotason virtualisointi (eng. hardware level virtualization) (Natawiguna & Liem, 2016). laitteistotason virtualisoinnissa samalla laitteella voidaan ajaa useita käyttöjärjestelmiä jakamalla käytössä olevat laitteistoresurssit, kuten suoritinteho, muisti, sekä kiintolevy, virtuaalikoneiden (eng. virtual machine) eli ohjelmallisesti tuotettujen tietokoneiden välillä. (NIST, 2011.) Virtuaalikone vastaa siis loogisesti fyysistä laitetta (Perakovic ym., 2014).

Virtuaalikoneet ovat eristettyinä toisistaan ja tiedonsiirto, sekä ohjelmien viestiminen voidaan estää isäntäkäyttöjärjestelmän (eng. host operating system) ja vieraskäyttöjärjestelmien (eng. guest operating system) välillä. Näin työntekijät voivat hoitaa omia henkilökohtaisia asioitaan erillään organisaation datasta ja ohjelmista. (Perakovic ym., 2014.) Palvelintasolla organisaatio voi jakaa tällä tavalla organisaation toimintoja ja ohjelmia erillisille virtuaalisille palvelimille (Jain & Choudhary, 2016). Vaikka nämä teknologiat kehitettiinkin alun perin toimimaan tietokoneissa ja palvelimilla, voidaan niitä hyödyntää nykyään myös mobiiliympäristössä (Jaramillo, Newhook & Nassar, 2014).

Laitteistotason virtualisointisovellusta, joka luo ja ajaa virtuaalikoneita, kutsutaan virtuaalikonemonitoriksi (eng. hypervisor tai virtual machine monitor). Virtuaalikonemonitoreja on kahdenlaisia: Tyypin 1 virtuaalikonemonitoreilla tarkoitetaan käytännössä käyttöjärjestelmäytimiä ja ne toimivat suoraan laitteistotasolla. Ne kontrolloivat laitteistoa ja sen päällä suoritettavia käyttöjärjestelmiä. Tyypin 2 virtuaalikonemonitorit sen sijaan ovat ohjelmistoja, jotka toimivat isäntänä toimivan käyttöjärjestelmän sisällä samaan tyyliin kuin mikä tahansa muukin ohjelmisto. Tyypin 1 virtuaalikonemonitoreja pidetään tehokkaampana kuin tyypin 2 virtuaalikonemonitoreja. (Timcenko, Djordjevic, Rakas & Davidovic, 2014.) Tyypin 1 virtuaalikonemonitoreja pidetään myös turvallisempina, koska siinä käyttöjärjestelmät ovat täysin eristettyinä toisistaan (Jaramillo, 2013, s. 10). Tyypin 2 virtuaalikonemonitoreissa hyökkääjä saattaa esimerkiksi hyökätä virtuaalikoneisiin isäntänä toimivan käyttöjärjestelmän kautta (Perakovic ym., 2014). Tyypin 2 virtuaalikonemonitoreissa virtualisoitujen käyttöjärjestelmien suorituskyky on myös riippuvainen isäntänä toimivasta käyttöjärjestelmästä, ja ongelmat isäntäkäyttöjärjestelmässä vaikuttavat myös vieras-

käyttöjärjestelmiin (Jaramillo, 2013, s. 10). Tyypin 1 virtuaalikonemonitorit kuluttavat kuitenkin enemmän suoritintehoa ja muistia (Mostefaoui & Tariq, 2018, s. 27).

Laitteistotason virtualisoinnissa on kuitenkin ongelmia erityisesti mobiilikäytössä. Kahden tai useamman käyttöjärjestelmäilmentymän käyttö samalla mobiililaitteella voi vaikuttaa laitteen suorituskykyyn. Työntekijät joutuvat lisäksi vaihtamaan eri käyttöjärjestelmäilmentyminen välillä riippuen siitä, hoitavatko he organisaation asioita vai omia henkilökohtaisia asioitaan. Tämä voi tuntua työntekijöistä epäkäytännölliseltä. (Perakovic ym., 2014.) Etenkin Tyypin 1 virtuaalikonemonitoreja käytettäessä vaihtaminen käyttöjärjestelmien välillä voi olla työlästä (Mostefaoui & Tariq, 2018, s. 27). Laitteistotason virtualisoinnin käyttöönotto voi olla myös laitteesta riippuen hyvin hankalaa esimerkiksi älypuhelimissa. Käyttöjärjestelmät on usein asennettu laitteisiin jo ennen niiden hankkimista, eivätkä valmistajat välttämättä salli useiden käyttöjärjestelmien asentamista. (Hovav & Putri, 2016.)

Kolmas virtualisoinnin muoto on käyttöjärjestelmätason virtualisointi (eng. operating system level virtualization). Käyttöjärjestelmätason virtualisoinnissa käyttöjärjestelmäydin mahdollistaa ohjelmistojen ajamisen useissa toisistaan eristetyissä käyttäjätiloissa. Näitä käyttäjätiloja kutsutaan usein säiliöiksi (eng. containers). (Jimenes ym., 2016.) Useat käyttäjätilat mahdollistavat organisaation ohjelmistojen ja datan eristämisen työntekijöiden ohjelmista ja datasta (Reshetova, Karhunen, Nyman & Asokan, 2014). Käyttöjärjestelmäydin tarjoaa usein resurssienhallintaominaisuuksia, jotta toiminta toisissa säiliöissä ei vaikuta muihin säiliöihin (Huang & Wu, 2017, s. 47).

Käyttöjärjestelmätason virtualisointi ei vaadi virtuaalikonemonitorien käyttämistä, vaan siinä hyödynnetään suoraan isäntäkäyttöjärjestelmää. Säiliöt sisältävät kaiken mitä ohjelmistojen ajamiseen tarvitaan, kuten tarvittavat järjestelmätyökalut, kirjastot ja asetukset. Virtuaalikoneisiin verrattuna säiliöt vievät vähemmän muistia ja levytilaa, sekä käynnistyvät huomattavasti nopeammin. (Silva, Kirikova & Alksnis, 2018.) Käyttöjärjestelmätason virtualisointi ei vaikuta myöskään niin paljoa laitteiden suorituskykyyn verrattuna laitteistotason virtualisointiin. Sen avulla voidaan lisäksi välttää ohjelmistojen päällekkäisyyttä. (Liu, Gu & Gu, 2017.) Cellrox on esimerkki käyttöjärjestelmätason virtualisointia hyödyntävästä teknologioista. Se mahdollistaa kahden tai useamman käyttäjätilan luomisen Andoid-laitteille. Yksi käyttäjätila voi olla esimerkiksi työntekijän henkilökohtaiseen käyttöön ja toinen työkäyttöön. Työnantaja pystyy valvomaan työkäyttöön tarkoitettua käyttäjätilaa, mutta työntekijän omat tiedot pysyvät suojassa hänen omassa käyttäjätilassaan. (Reshetova ym., 2014.)

Käyttöjärjestelmätason virtualisointi ei ole kuitenkaan yhtä joustavaa kuin laitteistotason virtualisointi, koska kaikilla vieraskäyttöjärjestelmillä tulee olla sama käyttöjärjestelmäydin kuin isäntäkäyttöjärjestelmällä. Jos isäntäkäyttöjärjestelmä on esimerkiksi Linux-pohjainen, erilaisia Linux-jakeluja voidaan käyttää, mutta ei esimerkiksi Windowsia. (Reshetova ym., 2014.) Koska käyttöjärjestelmätason virtualisoinnissa käyttöjärjestelmäydin jaetaan, säiliöt eivät myös-

kään ole yhtä hyvin eristettyinä toisistaan verrattuna virtuaalikoneisiin, eivätkä näin ollen yhtä turvallisia (Hovav & Putri, 2016).

5 YHTEENVETO

Tässä tutkielmassa selvitettiin minkälaisia tietoturvauhkia organisaatiot kohtaavat BYOD-ympäristössä ja miten ne toteutuessaan voivat vaikuttaa organisaatioon. Lisäksi tutkielmassa selvitettiin, millaisilla erilaisilla teknisillä ratkaisuilla tietoturvauhkia voidaan organisaatioissa hallita ja minkälaisia rajoitteita hallintakeinoihin liittyy. Tutkielma kirjoitettiin kirjallisuuskatsauksena ja lähdekirjallisuuden perusteella pyrittiin vastaamaan seuraaviin kysymyksiin:

- Minkälaisia tietoturvariskejä organisaatiot kohtaavat BYOD-ympäristössä ja mitä vaikutuksia niillä toteutuessaan on organisaatiolle?
- Minkälaisilla teknisillä ratkaisuilla BYOD-ympäristön aiheuttamia tietoturvariskejä voidaan organisaatioissa hallita ja mitä rajoitteita hallintakeinoihin liittyy?

Tutkielman toisessa luvussa selvitettiin, mitä BYOD-ilmiöllä oikeastaan tarkoitetaan käytännössä. Nimensä mukaisesti BYOD viittaa siihen, että työntekijät voivat tuoda omat mobiililaitteensa työpaikalleen, ja käyttää niitä työtarkoituksiin (Bello ym., 2017). BYOD sisältää käsitteenä kuitenkin myös mahdollisuuden hoitaa organisaation asioita myös työpaikan ulkopuolelta ja se mahdollistaa saman mobiililaitteen käytön myös henkilökohtaisiin tarpeisiin (Rivadeneira & Rodrigues, 2018). BYOD ei myöskään viittaa ainoastaan mobiililaitteeseen itseensä, vaan työntekijät voivat tuoda työpaikalle myös omat ohjelmistonsa ja palvelunsa (Morrow, 2012). BYOD on siis käsitteenä hyvin laaja. Toisessa luvussa käsiteltiin myös BYOD-ilmiön nykyistä tilaa, sekä sen aiheuttamia hyötyä työntekijöille ja organisaatioille.

Kolmannessa luvussa käsiteltiin tietoturvauhkia, joita organisaatiot kohtaavat BYOD-ympäristössä, sekä selvitettiin mitä vaikutuksia uhilla voi toteutuessaan olla organisaatoille. Organisaatiot kohtaavat BYOD-ympäristössä tietoturvauhkia, jotka yleisestekin koskettavat mobiililaitteita (Tse ym., 2016). Kuitenkin se tosiasia, että työntekijät käyttävät samoja mobiililaitteitaan niin työtarkoituksiin, kuin myös henkilökohtaiseen käyttöönsä, altistaa organisaation

datan erittäin suureen vaaraan. Tietoturvauhkia BYOD-ympäristössä käsittelevissä julkaisuissa esille nousivat haittaohjelmat, palvelunestohyökkäykset, sosiaalinen manipulointi, mobiililaitteiden häviäminen, sekä työntekijöistä itsestään johtuvat tietoturvariskit. Tässä tutkielmassa on pyritty käsittelemään tietoturvauhkia monipuolisesti, mutta johtuen aiheen laajuudesta, tutkielmassa pyrittiin kertomaan miksi uhat ovat merkittäviä juuri BYOD-kontekstissa. Kaikkien käsiteltyjen tietoturvauhkien vaikutusten keskiössä oli organisaation datan häviäminen tai varastaminen, tai organisaatioiden järjestelmien vaarantuminen työntekijöiden mobiililaitteiden vuoksi. Tietoturvauhat ja niiden mahdolliset vaikutukset organisaatiolle on tiivistetysti kuvattu taulukossa 1.

TAULUKKO 1 Tietoturvariskit ja niiden mahdolliset vaikutukset organisaatiolle.

Tietoturvariski	**Mahdolliset vaikutukset organisaatiolle**
Haittaohjelmat	• Organisaation datan vuotaminen ulkopuoliselle taholle (Olalere ym., 2015). • Organisaation sovellusten vahingoittuminen tai häiröt niiden toiminnassa (Olalere ym., 2015).
Palvelunestohyökkäykset	• Palvelujen käytön estyminen oikeudellisilta käyttäjiltä (Farina ym., 2015). • Häiriöt organisaation järjestelmien toiminnassa (Farina ym-, 2015). • Altistuminen muille tietoturvauhille (Olalere ym., 2015).
Sosiaalinen manipulointi	• Organisaation datan vuotaminen ulkopuoliselle taholle (Flores ym., 2016).
Mobiililaitteen katoaminen tai varkaus	• Organisaation datan vuotaminen ulkopuoliselle taholle (Morrow, 2012).
Mobiililaitteiden heikko suojaus ja huolimaton käyttö	• Kasvanut haittaohjelmatartunnan riski (Harris ym., 2013). • Organisaation datan vuotaminen ulkopuoliselle taholle (Bello ym., 2017).

Neljännessä luvussa käsiteltiin erilaisia teknisiä ratkaisuja, joita organisaatiot voivat käyttää uhkien hallinnassa. Tutkielmassa käytetyssä lähdekirjallisuudessa esiteltiin usein vain muutamia eri hallintakeinoja ja erityisesti mobiililaitehallintaa käsiteltiin monessa julkaisussa. Tässä tutkielmassa käsiteltiin mobiililaitehallintaa, mobiilisovellushallintaa, mobiilisisällön hallintaa ja näiden yhdistelmäratkaisuja, eli yrityksen mobiiliuden hallintaa. Lisäksi tutkielmassa käsiteltiin pääsynhallintaa tietoverkkoihin, sekä virtualisoinnin eri hyödyntämiskeinoja. Tutkielman neljännessä luvussa pyrittiin vastaamaan siihen, minkälaisilla eri teknologioilla BYOD-ympäristössä ilmeneviä tietoturvariskejä voidaan hallita, sekä minkälaisia rajoitteita eri hallintakeinoihin liittyy. Monipuolisista ominaisuuksista ja erilaisista lähestymistavoista huolimatta rajoitteita löytyi kaikista tutkielmassa käsitellyistä hallintakeinoista, eikä mikään niistä välttämättä riitä tarjoamaan riittävää suojaa tietoturvauhkia vastaan. Erilaiset hyök-

käykset myös kehittyvät jatkuvasti, eikä nykyratkaisuilla välttämättä pystytä suojautumaan esimerkiksi kehittyneitä bottiverkkoja vastaan (Eslahi ym., 2014). Tutkielmassa käsitellyt hallintakeinot, sekä niihin liittyvät rajoitteet on tiivistetysti kuvattu taulukossa 2.

TAULUKKO 2 Tietoturvariskien hallintakeinot, sekä niiden rajoitteet.

Hallintakeino	**Hallintakeinon rajoitteet**
Mobiililaitehallinta	• Mahdollisuus poistaa MDM-agentti mobiililaitteesta (Alotaibi & Almagwashi, 2018). • Rajoitettu liitettävien laitteiden määrä (Alotaibi & Almagwashi, 2018). • Mahdollisuus organisaation ja työntekijän datan sekoittumiseen (Alotaibi & Almagwashi, 2018). • Vaatii kolmansien osapuolien sovellusten asentamista (Alotaibi & Almagwashi, 2018). • Ei mahdollisuutta hallita laitetta täysin vianmääritystä varten (Garba ym., 2015).
Mobiilisovellushallinta	• Kykenee hallitsemaan ainoastaan tiettyjä ennalta määriteltyjä sovelluksia (Scarfo, 2012).
Mobiilisisällön hallinta	• Organisaation datan käsittely ja hallinta on mahdollista vain tietyissä ennalta määritellyissä palveluissa (Eslahi ym., 2014).
Yritysten mobiiliuden hallinta	• Yhdistää muiden hallintajärjestelmien rajoitteita (Alotaibi & Almagwashi, 2018). • Ei tarjoa välttämättä riittävää suojaa kehittyneitä hyökkäyksiä vastaan (Eslahi ym., 2014)
Pääsynhallinta tietoverkkoihin	• Ei mahdollisuutta valvoa ja kontrolloida laitteita verkkoon liittymisen jälkeen (Kim & Kim, 2015). • Multimediasisällön hallinta saattaa johtaa verkon ylikuormittumiseen (Garba ym., 2015). • Käyttöoikeuksien määrittäminen voi olla hankalaa, varsinkin jos käyttäjällä on verkossa useita eri laitteita (Garba ym., 2015). • Haittaohjelmat saattavat levitä virtuaalilähiverkoissa (Garba ym., 2015). • Virtuaalisten erillisverkkojen käyttäjät saattavat vaarantaa organisaation tietoverkon (Garba ym., 2015).
Virtualisointi:	
Virtuaalinen työasemaympäristö	• Joidenkin ohjelmistojen käyttö vaikeaa tai mahdotonta muun muassa näppäimistön puutteen vuoksi (Perakovic ym., 2014). • Mobiililaitteiden pienen koon vuoksi esimerkiksi sovellusten alasvetovalikot saattavat jäädä kuvaruudun ulkopuolelle (Perakovic ym., 2014).

(jatkuu)

Taulukko 2 (jatkuu)

Laitteistotason virtualisointi	Tyyppi 1	• Kuluttaa tyypin 2 virtuaalikonemonitoreihin verrattuna enemmän suoritintehoa, sekä muistia. (Mostefaoui & Tariq, 2018, s. 27). • Saattaa vaikuttaa laitteen suorituskykyyn (Perakovic ym., 2014). • Käyttöjärjestelmien välillä vaihtaminen voi olla työlästä (Mostefaoui & Tariq, 2018, s. 27). • Käyttöönotto voi olla laitteesta ja käyttöjärjestelmästä riippuen vaikeaa (Hovav & Putri, 2016).
Laitteistotason virtualisointi	Tyyppi 2	• Tyypin 1 virtuaalikonemonitoreihin verrattuna tehottomampi ja käyttöjärjestelmät ovat huonommin eristettyinä toisistaan (Jaramillo, 2013, s. 10). • Mahdollista hyökätä vieraskäyttöjärjestelmiin isäntäkäyttöjärjestelmän kautta (Perakovic ym., 2014). • Vieraskäyttäjärjestelmien toiminta on riippuvaista isäntäkäyttöjärjestelmästä (Jaramillo, 2013, s. 10). • Käyttöönotto voi olla laitteesta ja käyttöjärjestelmästä riippuen vaikeaa (Hovav & Putri, 2016). • Käyttö saattaa vaikuttaa laitteen suorituskykyyn (Perakovic ym., 2014).
Käyttöjärjestelmätason virtualisointi		• Ei mahdollista sellaisten käyttöjärjestelmien hyödyntämistä, jotka käyttävät eri käyttöjärjestelmäydintä (Reshetova ym., 2014). • Organisaation data ja käyttäjän data ovat huonommin eristettyinä toisistaan verrattuna laitteistotason virtualisointiin (Hovav & Putri, 2016).

Tämän tutkielman aihe oli hyvin monipuolinen ja tästä syystä asioita käsiteltiin varsin yleisellä tasolla. Esimerkiksi erilaisten organisaatiota vastaan kohdistuvien hyökkäysten kuvaaminen jäi pintapuoliseksi. Tutkielmassa ei myöskään vertailtu erilaisia kaupallisia ratkaisuja, vaan eri teknologioiden ominaisuuksia ja rajoitteita käsiteltiin yleisellä tasolla. BYOD-käsitteessä viitataan usein työntekijöiden mahdollisuuteen käyttää itse valitsemiaan mobiililaitteita. Tässä tutkielmassa ei kuitenkaan tarkasti käsitelty eri teknologioiden soveltumista eri mobiililaitteille. Käytännössä kaikkia esiteltyjä teknologioita ja niihin liittyviä ratkaisuja ei voida soveltaa kaikissa käyttöjärjestelmissä ja laitteissa. Myös Gaff (2015) esittää, että organisaatioiden pitää todennäköisesti jollain tasolla rajoittaa, mitä laitteita työntekijät saavat käyttää.

Tutkielmassa viitattiin mobiililaitteina kannettaviin tietokoneisiin, tabletteihin ja matkapuhelimiin. Tutkielmassa ei käsitelty miten esimerkiksi uudenlaiset IOT-laitteet voivat vaikuttaa organisaation tietoturvaan ja sen hallintaan. Tutkielma ei myöskään käsitä läheskään kaikkia BYOD-ympäristössä ilmeneviä tietoturvauhkia tai mobiiliturvallisuuden hallintaan käytettyjä teknologioita.

Tässä tutkielmassa tietoturvauhkia ja niiden hallintakeinoja käsiteltiin organisaation näkökulmasta. Tämä oli tavallista myös käyttämässäni lähdekirjallisuudessa, mutta myös asiaa työntekijän näkökulmasta käsitteleviä julkaisuja löytyi (mm. Hovav & Putri, 2016). En kuitenkaan löytänyt tutkimuksia, joissa olisi käsitelty sitä, miten BYOD-riskien hallintakeinot vaikuttavat omien mobiililaitteiden käytöstä aiheutuviin hyötyihin. Jotkin hallintateknologiat, kuten mobiililaitehallinta, mahdollistavat varsin vahvan kontrollin työntekijöiden mobiililaitteisiin ja joissakin teknologioissa, kuten mobiilisisällön hallinnassa, rajoitettiin työntekijöiden mahdollisuutta esimerkiksi jakaa tiedostoja tai käyttää tiettyjä ohjelmia. Tämä saattaa hyvinkin vaikuttaa myös hyötyihin, joita BYOD organisaatioille aiheuttaa ja tätä tulisi mielestäni tulevaisuudessa tutkia enemmän.

LÄHTEET

Aliyu, A., Danjuma, S., Dai, B., Waziri, U., Ado, A. (2014). An Integrated Framework for Detecting and prevention of Trojan Horse (BINGHE) in a Client-Server Network***. International Journal of Innovative Research in Science, Engineering and Technology***, 3(1), 8709-8716.

Alotaibi, B. & Almagwashi, H. (2018). A Review of BYOD Security Challenges, Solutions and Policy Best Practices. Teoksessa ***2018 1st International Conference on Computer Applications & Information Security*** **(ICCAIS**) (1-6). Riuadh, Saudi Arabia, April 4-6, 2018.

Alwahedi, S., Ali, M., A., Ishowo-Oloko, F., Woon, W., L. & Aung, Z. (2017). Security of Mobile Computing: Attack Vectors, Solutions and Challenges. Teoksessa Aguero, R., Zaki, Y., Wenning, B.-L., Förstrer, A. & Timm-Giel, A. (Toim.) ***Mobile Networks and Management. 8th International Conference (MONAMI)*** (177-191) Abu Dhabi, United Arab Emirates, October 23-24, 2016.

Belanger, F. & Crossler, R., E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. ***The Journal of Strategic Infoemation Systems***, 28(1), 34-49.

Bello, A.G., Murray, D. & Armarego, J. (2017), A systematic approach to investigating how information security and privacy can be achieved in BYOD environments***, Information and Computer Security***, 25(4), 475-492.

Concepcion, J., Chua, J., Siy, G. & Ballon, A. (2015). Securing Android BYOD(Bring Your Own Device) with Network Access Control(NAC) and MDM(Mobile Device Management). Teoksessa ***Proceedings of the DLSU Research Congress vol. 3 2015***, Manila, Philippines, March 2-4, 2015.

Dell & Intel (2011). The Evolving Workforce: The Business Perspective and Research Summary. Part 1: People. Haettu osoitteesta https://i.dell.com/sites/csdocuments/Corporate_secure_Documents/en/Evolving-Workforce-Report-3-People.pdf.

Dernbecher, S., Beck, R. & Weber, S. (2013). Switch to your own to work with the known: An empirical study of consumerization of IT. Teoksessa ***Proceedings of the 19th Americas Conference on Information Systems (AMCIS)***, Chicago, IL, USA, August 15-17, 2013.

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD***). Procedia Computer Science***, 78, 179-184.

Disterer, G. & Kleiner, C. (2013). BYOD Bring Your Own Device. ***Procedia Technology***, 9, 43-53.

Farina, P., Cambiaso, E., Papaleo, G. & Aiello, M. (2015). Understanding DDoS Attacks from Mobile Devices. Teoksessa ***3rd International Conference on Future Internet of Things and Cloud***, 614-619, Rome, Italy, August 24-26, 2015.

Flores, D., Jhumka, A. & Qazi, F. (2016). Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information. Teoksessa ***The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom)*** (1008-1015), Tianjin, China, August 23-26, 2016.

Gaff, B. M. (2015). BYOD? OMG!. ***Computer***, 48(2), 10-11.

Gajar, P., K., Ghosh, A. & Rai, S. (2013). BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES. ***Journal of Global Research of Computer Science***, 4(4), 62-70.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments***. Journal of Information Privacy & Security***, 11(1), 38-54.

Gartner. (31.07.2012). Hype Cycle for Emerging techologies, 2012. Haettu osoitteesta: https://www.gartner.com/doc/2100915.

Hameed, A. & Mian, A., N. (2012). Finding efficient VLAN topology for better broadcast containment. Teoksessa ***2012 Third International Conference on The Network of the Future (NOF)***, Gammarth, Tunisia, November 21-23, 2012.

Harris, M., A., Patten, K. & Regan, E. (2013). The need for BYOD mobile device security awareness and training. Teoksessa ***Proceedings of the Nineteenth Americas Conference on Information Systems (AMCIS),*** Chicago, Illinois, August 15-17, 2013.

Horalek, J., Matyska, J. & Sobeslav, V. (2013). Performance comparison of selected virtualization platforms. Teoksessa ***2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI)*** (327-332), Budapest, Hungary, Novermber 19-21, 2013.

Hohav, A. & Putri, F., F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. ***Pervasive and Mobile Computing***, 32, 35-49.

Huang, D. & Wu, H. (2017). ***Mobile Cloud Computing. Foundations and Service Models***. Cambridge: Elsevier. Haettu osoitteesta https://books.google.fi/books?id=dupGDgAAQBAJ&pg=PA303&dq=Huang+Lu+2017+containerization&hl=fi&sa=X&ved=0ahUKEwj9yt_MwbPpAhXuAhAIHYSjAoAQ6AEITjAE#v=onepage&q=Huang%20Lu%202017%20containerization&f=false.

Intel. (2011). Benefits of Enabling Personal Handheld Devices in the Enterprise. Haettu osoitteesta https://www.intel.co.za/content/dam/doc/best-practices/inte-it-it-leadership-benefits-of-enabling-personal-handheld-devices-in-the-enterprise-practices.pdf.

Jain, N. & Choudhary, S. (2016). Overview of virtualization in cloud computing. Teoksessa ***2016 Symposium on Colossal Data Analysis and Networking (CDAN)*** (1-4), Indore, India, March 18-19, 2016.

Jaramillo, D. (2013). VIRTUALIZATION TECHNIQUES FOR MOBILE SYSTEMS. (Väitöskirja, Florida Atlantic University). Haettu osoitteesta https://fau.digital.flvc.org/islandora/object/fau%3A13072/datastream/OBJ/view/Virtualization_techniques_for_mobile_systems.pdf.

Jaramillo, D., Newhook, R. & Nassar, N. (2014). Techniques and real world experiences in mobile device security. Teoksessa ***IEEE SOUTHEASTCON 2014***. ***(SECON)*** (1-6), Lexington, KY, USA, March 13-16, 2014.

Jimenez, I., Maltzan, C., Lofstead, J., Moody, A., Mohror, K., Arpaci-Dusseau, R. & Arpacu-Dusseau, A. (2016). Characterizing and Reducing Cross-Platform Performance Variability Using OS-Level Virtualization. Teoksessa ***2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*** (1077-1080), Chigago, IL, USA, May 23-27, 2016.

Kim, S. & Jin, H. (2015). A Simple Security Architecture for Mobile Office. ***International Journal of Security and its Applications***, 9(1), 139-145.

Kim, T. & Kim, H. (2015). A system for detection of abnormal behavior in BYOD based on web usage patterns. Teoksessa ***2015 International Conference on Information and Communication Technology Convergence (ICTC)*** (1288-1293), Jeju, South Korea, October 28-30, 2015.

Knackmuß, J. & Creutzburg, R. (2015). Enterprise Mobility Management (EMM) – a way to increase security of mobile devices. Teoksessa Creutzburg, R. & Akopian, D. (toim.) ***Proceeding of Spie: Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2015.***

Koh, E., B., Oh, J. & Im, c. (2014). A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment.

Teoksessa ***Proceedings of the International MultiConference of Engineers and Computer Scientists 2014 Vol II (IMECS***), Hong Kong, China, March 12 - 14, 2014.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015). Advanced Social Engineering Attacks. ***Journal of Information Security and Applications***, 22, 113-122.

Lakbabi, A. (2012). Network Access Control Technology—Proposition to Contain New Security Challenges**.** ***International Journal of Communications, Network and System Sciences***, 5(8), 505-512.

La Polla, M., N., Martinelli, F. & Sgandurra, D. (2013). A Survey on Security for Mobile Devices. ***IEEE Communications Surveys & Tutorials***, 15(1), 446-471.

Leavitt, N. (2013). Today's mobile security requires a new approach. ***Computer***, 46(11), 16-19.

Lebek, b., Degirmenci, K. & Breitner M., H. (2013). Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices. Teoksessa Shim, J P, Hwang, Y, & Petter, S (Toim.) ***Proceedings of the Nineteenth Americas Conference on Information Systems*** (***AMCIS***) (1-8). Chigago, Illinois, August 15-17, 2013.

Liotta, A., Tyrode-Goilo, D., H. & Oredope, A. (2007). Open Source Mobile VPNs over Converged All-IP Networks. ***Journal of Network and System Management***, 16, 163-181.

Liu, B.-W., Gu, N.-J, & Gu, D.H. (2017). A Lightweight OS-Level Virtualization Architechture Based on Android. Teoksessa ***2017 2nd International Conference on Computer, Network Security and Communication Engineering (CNSCE),*** Bangkok, China, March 26-27, 2017.

Meske, C., Stieglitz, S., Brockmann, T. & Ross, B. (2017). Impact of Mobile IT Consumerization on Organizations – An Empirical Study on the Adoption of BYOD Practices. Teoksessa Nah, F., H. & Tan, C., H. (toim.) ***HCI in Business, Government and Organizations. Supporting Business***, HCIBGO 2017 (349-363). Vancouver, BCM, Canada, July 9-14, 2017.

Miller, K., W., Voas, J. & Hurlburt, G., F. (2012). BYOD: Security and Privacy Consedirations. ***IT Professional***, 14(5), 53-55.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. ***Network Security***, 2012(12), 5-8.

Mostefaoui, G., K. & Tariq, F. (2018). ***Mobile Apps Engineering: Design, Development, Security, and Testing***. CRC Press.

Musa, A., Muhammed, M., A. & Ayesh, A. (2019). A Behaviour Profiling Based Technique for Network Access Control Systems. ***International Journal of Cyber-Security and Digital Forensics***, 8(1), 23-30.

National Institute of Standard and Technology. (2011***). Guide to Security for Full virtualization Technologies (Special Publication 800-125***) Haettu osoitteesta https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=907776.

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization - A Theory and Practice Review. Teoksessa ***Proceedings of the Eighteenth Americas Conference on Information Systems (AMCIS)*** *(9-12)*. Seattle, Washington, August 9-12, 2012.

Olalere, M., Abdullah, M. T., Mahmod, R. & Abdullah, A. (2015). A review of bring your own device on security issues. ***SAGE Open***, 5(2).

Oluwatimi, O., Midi, D. & Bertino, E. (2017). Overview of Mobile Containerization Approaches and Open Research Directions. ***IEEE Security & Privacy***, 15(1), 22-31.

Ophoff, J. & Miller, S. (2019). BUSINESS PRIORITIES DRIVING BYOD ADOPTION: A CASE STUDY OF A SOUTH AFRICAN FINANCIAL SERVICES ORGANIZATION. ***Issues in Informing Science + Information Technology***, 16, 165-196.

Palanisamy, R., Norman, A. A. & Mat Kiah, M. L. (2020). BYOD policy compliance: Risks and strategies in organizations. ***Journal of Computer Information Systems***, 1-12.

Peng, S., Yu, S. & Yang, A. (2014). Smartphone Malware and Its Propagation Modeling: A Survey. ***IEEE Communications Surveys & Tutorials,*** 16(2), 925-941.

Perakovic, D. & Husnjak, S. & Cvitic, I. (2014). Comparative analysis of enterprise mobility management systems in BYOD environment. Teoksessa ***The 2nd Research Conference In Technical Disciplines (RCITD)*** (76-81), Dubna, Slovakia, Novermber 17-21, 2014.

Pierer, M. (2016). ***Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises***. Vienna: Springer. Haettu osoitteesta https://books.google.fi/books?id=S6HVDAAAQBAJ&printsec=frontcover&hl=fi&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

Prowse, D., L. (2015). Learn, Prepare and Practise for Exam Success. ***CompTIA Security+ SY0-401 Cert Guide, Academic Edition: Comp Secu SY04.***

Rababah, B., Zhou, S. & Bader, M. (2018). Evaluation the Performance of DMZ. ***International Journal of Wireless and Microwave Technologies,*** 1(1), 1-13.

Reshetova, E., Karhunen, J., Nyman, T. & Asokan, N. (2014). Security of OS-Level Virtualization Technologies. Teoksessa Bernsmed, K. & Fischer-Hübner, S. (toim.***) Secure IT Systems. Lecture Notes in Computer Science***, NordSec 2014 (77-93). Cham: Springer.

Rhee, K., Won, D., Jang, S.-W., Chae, S. & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. ***Electronic Commerce Research***, 13, 243-256.

Rivadeneira, F., R. & Rodrigues, G., D. Bring your own device: a survey of threats and security management models***. International Journal of Electronic Business***, 14(2), 146.

Romer, H. (2014). Best practises for BYOD scurity. ***Computer Fraud & Security***, 1, 13-15.

Rose, C. (2013). BYOD: An Examination Of Bring Your Own Device In Business. ***Review of Business Information Systems***, 17(2), 65-70.

Saari, L., M. & Judge, T., A. (2004). Employee attitudes and job satisfaction. ***Human recourse management***, 43(4), 395-407.

Sahriah, H., Klintic, T. & Clincy, V. (2015). Mobile Phishing Attacks and Mitigation Techiques. ***Journal of Information Security***, 6, 206-212.

Scarfo, A. (2012). New Security Perpectives around BYOD**.** Teoksessa ***Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA),*** 446-451, Victoria, BC, Canada November 12-14, 2012.

Silva, V., G., D., Kirikova, M. & Alksnis, G. (2018). Containers for Virtualization: An Overview. ***Applied Computer Systems,*** 23(1), 21-27.

Syntonic. (2016). Syntonic 2016 Employer report: BYOD Usage in the Enterprise. Haettu osoitteesta https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf.

Tatte, G. & Bamnote, G., R. Mobile Device Management A Functional Overview. ***International Journal of Computer Science and Applications***, 6(2), 319-323.

Thomson, G. (2012). BYOD: Enabling the chaos**.** ***Network Security***, 2012(2). 5-8.

Timchenko, V., Djordjevic, B., Rakas, S., B. & Davidovic, N. (2014). Teoksessa ***2014 Proceedings of International Conference, Information Systems and Design of Communication (ISDOC)*** (122-126), Lisbon, Portugal, May 16-17, 2014.

Tse, D., Wang, L. & Li, Y. (2016). Mobility management for enterprises in BYOD deployment. Teoksessa ***The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom)*** (638-645), Tianjin, China, August 23-26, 2016.

Tu, Z., Yuan, Y. & Archer, N. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft***. International Journal of Mobile Communications***, 12(6), 603-623.

Vignesh, U. & Asha, S. (2015). Modifying Security Policies Toward BYOD. ***Procedia Computer Science***, 50, 511-516.

Weeger, A., Wang, X. & Gewald, H. (2015). It Consumerization: Byod-Program Acceptance and its Impact on Employer Attractiveness***. Journal of Computer Information Systems***, 56(1), 1-10.

Wu, F., Narang, H. & Clarke, D. (2014). An Overview Of Mobile Malware and Solutions. ***Journal of Computer and Communications***,2, 8-17.

Yuvaraj, D., Sivaram, M., Ayoobkhan, M. & Nageswari, S. (2019). Some Investigation on DDOS Attack Models in Mobile Networks***. International Journal of Interactive Mobile Technologies***, 13(10), 71-88.

Zahadat, N., Blessner, P., Blackburn, T. & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis***. Computers and Security***, 50, 81-99.

.