Haaga-Helia
ammattikorkeakoulu Oy

# Esineiden internet suomalaisissa pk-yrityksissä tietoturvan näkökulmasta

Juha-Pekka Pulkkinen

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2021

**Tiivistelmä**

Haaga-Helia
ammattikorkeakoulu Oy

**Tekijä(t)**
Juha-Pekka Pulkkinen

**Koulutusohjelma**
Tietojenkäsittelyn koulutusohjelma

**Raportin/Opinnäytetyön nimi**
Esineiden internet suomalaisissa pk-yrityksissä tietoturvan näkökulmasta

**Sivu- ja liitesivumäärä**
49 + 0

Tämä tutkimustyyppinen opinnäytetyö on toteutettu laadullisin menetelmin. Työssä tutkitaan esineiden internetiä suomalaisissa pk-yrityksissä tietoturvan näkökulmasta, sisältöanalyysin menetelmiä soveltaen. Tutkittavan asian nykytilannetta on pyritty kartoittamaan käyttäen tähän tarkoitukseen kerättyä dokumenttiaineistoa. Lähdeaineistona tässä työssä on käytetty erilaisia aiheeseen liittyviä artikkeleita, kirjallisuuslähteitä, blogijulkaisuja, verkkojulkaisuja ja muita vastaavia lähteitä. Opinnäytetyön ajankohtaisuuden takaamiseksi, tietoa on haettu mahdollisimman ajan tasalla olevista ja luotettavista lähteistä.

Työ on rajattu niin, että siinä keskitytään tarkastelemaan esineiden internetin tämänhetkistä tilannetta vain suomalaisten pk-yritysten kohdalla. Työssä ei ole tutkittu mitään tiettyä yksittäistä tietoturvaratkaisua tai innovaatiota, vaan siinä on pyritty tutkimaan esineiden internetin tietoturvaa laajempana kokonaisuutena.

Esineiden internet on kovaa vauhtia kasvava teknologiasuuntaus, joka on luonut ympärilleen paljon yleistä kiinnostusta. Se on teknologiasuuntaus, jota hyödyntämällä moni yritys pyrkii hakemaan itselleen parempaa kilpailukykyä ja kustannussäästöjä. Uusi hyödynnettävä teknologia kuitenkin tuo aina mukanaan myös uusia riskejä, joihin pitää pystyä vastaamaan hyvien käytänteiden ja tietoturvasuunnittelun kautta. Tällöin on tiedettävä miltä uhkilta ja riskeiltä tulee osata suojautua ja kuinka tunnistettuja ja tunnistamattomia uhkia vastaan voidaan varautua tehokkaasti. Tämän opinnäytetyön tulokset auttavat ymmärtämään edeltävää kokonaisuutta paremmin ja mahdollistavat osaltaan parempaa päätöksentekoa tulevaisuudessa.

Oikeanlaisella tietoturvasuunnittelulla, sisäisten dokumenttien laatimisella ja ylläpidolla, kattavalla ja jatkuvalla seurannalla, hyvien yhteistyökumppaneiden valinnalla sekä yleisten hyvien tietoturvakäytänteiden noudattamisella voidaan minimoida tehokkaasti riskejä, jotka voivat suoraan tai epäsuorasti vaikuttaa muuten negatiivisesti esineiden internetin järjestelmiin ja laiteratkaisuihin.

Työ on toteutettu keväällä 2021.

**Asiasanat**
Esineiden internet, pienet ja keskisuuret yritykset, tietoturva, pilvipalvelut, digitalisaatio

## Sisällys

# 1 Johdanto

Esineiden internet on jatkuvasti kasvava ja kehittyvä teknologiasuuntaus, joka on luonut ympärilleen paljon yleistä kiinnostusta. Sitä sovelletaan tällä hetkellä varsinkin valmistavassa teollisuudessa ja kuluttajille tarjottujen älylaitteiden kanssa. Keskeisenä piirteenä esineiden internetissä ovat tietoverkkojen ja analytiikan hyödyntäminen.

Yhteiskunnassa tapahtuva digitalisaatio aiheuttaa painetta yrityksille soveltaa uusia teknologioita, joiden kautta pyritään saavuttamaan parempaa kilpailukykyä markkinoilla ja synnyttämään kustannussäästöjä yritysten sisällä. Juuri tähän tarkoitukseen esineiden internetin erilaisia ratkaisuja pyritään soveltamaan ja kyseinen trendi ei ole yleistynyt ainoastaan suurten toimijoiden keskuudessa, vaan myös pk-yrityksissä maailman laajuisesti. Nämä uudet teknologiat ja ratkaisut tuovat mukanaan uusia mahdollisuuksia niitä hyödyntäville yrityksille, mutta ne myös tuovat mukanaan uusia riskejä, joihin pitää pystyä vastaamaan hyvien käytänteiden ja tietoturvasuunnittelun avulla. Siksi on tärkeää, että näissä yrityksissä ymmärretään paremmin, mistä nämä uhkat koostuvat ja kuinka niitä voidaan mahdollisesti torjua tai niihin liittyviä ongelmia ennaltaehkäistä tehokkaasti. Tämän opinnäytetyön tulokset auttavat ymmärtämään edeltävää kokonaisuutta paremmin ja mahdollistavat osaltaan parempaa päätöksentekoa tulevaisuudessa.

Pienillä ja keskisuurilla yrityksillä on Euroopan Unionin ja Suomen talouden kannalta merkittävä asema, sillä ne muodostavat näiden taloudellisen selkärangan. Kuitenkin pk-yrityksillä itsellään on vain rajattu määrä resursseja käytettävissään, joka luonnollisesti tarkoittaa sitä, että nämä resurssit tulee käyttää järkevästi. Tietoturvaa ei kuitenkaan tule unohtaa, varsinkaan esineiden internetin kanssa, sillä tietoturvan pettämisellä saattaa olla taloudellisia ja muita vakavia seurauksia yrityksille, heidän sidosryhmilleen sekä asiakkailleen.

Esineiden internet ja siihen liittyvä tietoturva on varsin ajankohtainen aihe opinnäytetyölle, koska elämme parhaillaan murrosvaiheessa, jossa esineiden internet ei ole vielä saavuttanut täyttä kypsyyttä teknologiselta kannalta katsottuna.

Tämä tutkimustyyppinen opinnäytetyö on toteutettu laadullisin menetelmin. Kyseessä on kirjallisuuskatsaus, jossa tutkitaan esineiden internetiä suomalaisissa pk-yrityksissä tietoturvan näkökulmasta sisältöanalyysin menetelmiä hyväksikäyttäen. Tutkittavan asian nykytilannetta on pyritty kartoittamaan käyttäen tähän kerättyä dokumenttiaineistoa. Aineistona tässä työssä on käytetty erilaisia aiheeseen liittyviä artikkeleita, kirjallisuuslähteitä, blogijulkaisuja, verkkojulkaisuja ja muita vastaavia lähteitä. Lähteinä on pyritty käyttämään

mahdollisimman luotettavaa materiaalia, joten sitä on haettu Haaga-Helian kirjaston tarjoamien palveluiden kautta, mutta myös muualta julkisesta verkosta tarvittaessa.

Tässä opinnäytetyössä on selvitetty dokumenttiaineiston pohjalta kolmea tutkimuskysymystä, joista kaksi jälkimmäistä ovat toissijaisia verrattuna ensimmäiseen pääkysymykseen.

- Mitä tunnistettavia tietoturvariskejä ja ehkäisykeinoja pk-yritysten tulisi huomioida esineiden internetin suhteen? Eli mitä tulee huomioida tietoturvasuunnittelussa esineiden internetiä hyödynnettäessä pk-yritysympäristössä, sekä kuinka näihin uhkiin voidaan varautua.

- Minkälaista tietoturvasuunnittelua pk-yrityksissä tulisi noudattaa esineiden internetin kanssa? Eli mistä hyvä suunnittelu lähtee ja mitä se ottaa huomioon, jotta tietoturvasuunnittelu olisi tarpeeksi onnistunutta kattamaan tietoturvatarpeet pk-yrityksissä esineiden internetin suhteen.

- Mikä on pk-yritysten ja esineiden internetin teknologia- ja tietoturvatilanne nyt? Eli mikä on tämänhetkinen tilanne juuri pk-yritysten kohdalla, kun mietitään laajemmin niiden tilannetta esineiden internetin ja siihen liittyvän tietoturvan suhteen sekä mitä teknologioita hyödynnetään tällä hetkellä.

Opinnäytetyö on rajattu niin, että siinä keskitytään tarkastelemaan esineiden internetin tämänhetkistä tilannetta ja tietoturvaa ainoastaan suomalaisten pk-yritysten kannalta. Työssä ei tarkastella mitään tiettyä yksittäistä tietoturvaratkaisua tai innovaatiota, vaan siinä pyritään toteuttamaan katsaus esineiden internetin tietoturvaan laajempana kokonaisuutena.

Oheisessa taulukossa 1 on koottuna käsitteitä, jotka ovat opinnäytetyön luettavuuden kannalta tärkeitä ymmärtää.

| Käsite | Määritelmä |
|---|---|
| Internet of Things (IoT) | Suomeksi esineiden internet, on toisiinsa kytkettyjen tunnistettavissa olevien laitteiden ja esineiden muodostama verkko. Esineiden internet on myös niin kutsuttu ylätason käsite kyseisestä teknologiasta. |
| Industrial Internet of Things (IIoT) | Teollinen esineiden internet on koneiden, tietokoneiden ja ihmisten internet, joka mahdollistaa älykkään teollisen toiminnan data-analytiikan avulla. |
| Internet of Everything (IoE) | Kaiken internet, on käytännössä vaihtoehtoinen termi ylätason käsitteelle esineiden internet. |
| Industrie 4.0 | Teollisuus 4.0 -käsitettä käytetään joissain maissa kuvaamaan varsinkin valmistavassa teollisuudessa käytettyä teollista esineiden internetiä. |
| NoSQL | Relaatiotietomallista poikkeava tietokantatyyppi, joka soveltuu hyvin massadatan tallennukseen. |
| Hadoop | Massadatan tallennukseen käytetty palvelinryppääseen eli klusteriin perustuva hajautettu tallennusjärjestelmä. |
| Big Data | Massadata -käsite kuvaa jatkuvasti kasvavaa massiivista tietojoukkoa |
| Data mining | Suomennettuna tiedonlouhinta, kuvaa joukkoa erilaisia menetelmiä, joiden avulla massadatasta pyritään löytämään juuri tiettyjä haluttuja tietoja. |
| Blockchain | Suomennettuna lohkoketju, on eräänlainen vahvasti suojattu linkitetyistä datalohkoista koostuva hajautettu tietokanta. |
| Pk-yritys | Käsitteellä viitataan pieniin ja keskisuuriin yrityksiin, joissa on alle 250 työntekijää. |
| IoT-yhdyskäytävä | Esineiden internetin ratkaisujen yhteydessä käytetty laite, joka yhdistää yksityisen verkon ja internetin. |

Taulukko 1. Opinnäytetyöhön liittyvien käsitteiden määritelmät.

# 2 Määritelmät

Tässä luvussa käydään läpi erilaisia määritelmiä, jotka ovat tärkeitä opinnäytetyön aiheen kannalta. Tässä luvussa myös luodaan raamit kokonaisuudelle, jota työssä tutkitaan. Luvussa myös havainnoidaan, miten esineiden internet liittyy teknologiseen kehitykseen ja miksi siihen ollaan siirtymässä. Luku on osa tietoperustaa, jonka varaan myöhempi empiirinen osio nojaa. Luvussa on myös esitetty havaintoja ja johtopäätöksiä lähdemateriaalien pohjalta.

## 2.1 Tietoturvallisuus

Tietoturvallisuus, eli yleisesti kutsuttuna tietoturva on käsitteenä laaja ja tämän opinnäytetyön kannalta erittäin keskeinen asia. Tietoturvasta puhuttaessa se voidaan määrittää monella eri tavalla ja hahmottaa monelta eri kantilta. Suomessa valtiovarainministeriö on antanut asiasta myös omia päätöksiään, jotka on suunnattu enemmän sen alaisille tahoille, mutta niissä on myös yleispäteviä kirjauksia, liittyen juuri tietoturvaan ja sen määritelmään.

> Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta. (Valtiovarainministeriö 2009, 26–27)

Tietoturvallisuuden keskeiset käsitteet ovat siis luottamuksellisuus, eheys, käytettävyys, todentaminen ja kiistämättömyys. Luottamuksellisuudella viitataan siihen, että tiedot ja järjestelmät ovat vain luotettujen tahojen tai henkilöiden käytettävissä, eli nämä tahot ovat saaneet oikeudet asiaan. Ulkopuoliset tahot eivät voi muuttaa, käsitellä tai tuhota mitään tietoihin tai järjestelmiin liittyvää, koska he eivät ole luotettuja tahoja ja heillä ei ole tarvittavia oikeuksia. Eheys tarkoittaa tässä yhteydessä, että tietojen ja järjestelmien luotettavuus on säilynyt ja ne eivät sisällä tahallisia tai tahattomia muokkauksia tai virheitä. Käytettävyys viittaa siihen, että tiedot ja palvelut ovat oikeutettujen tahojen tai henkilöiden saatavilla tarvittuna ajankohtana ja käytettävässä muodossa. Todentamisella, eli autentikoinnilla tarkoitetaan eri osapuolten luotettavaa tunnistamista, olivat ne sitten järjestelmiä tai henkilöitä. Kiistämättömyys tarkoittaa tässä yhteydessä tapahtuneen asian todentamista jälkikäteen. Sillä varmennetaan, ettei osallinen taho voi kiistää toimintaansa missään vaiheessa, koska suoritetuista tapahtumista jää merkintä. (Valtiovarainministeriö 2009, 26–27)

Valtiovarainministeriön vuonna 2009 antama määritelmä tietoturvasta ja sen keskeisistä käsitteistä ovat erittäin päteviä ja olennaisia edelleen. Nämä määritelmät ovat tunnistettavissa olevia asioita ja käytettävissä kulloinkin sovellettavasta teknologiasta riippumatta.

Tietoturvasta puhuttaessa törmää vääjäämättä myös termiin kyberturvallisuus, jota käytetään nykyään hyvin laajalti kuvaamaan erilaisia tietoturvallisuuteen liittyviä käytäntöjä. Tässä opinnäytetyössä on tarkoitus tarkastella asioita juuri tietoturvan näkökulmasta, mutta lukijan on syytä huomioida, että kyberturvallisuudessa on kyse samasta ilmiöstä. Varsinkin Suomessa on muodostunut eräänlaiseksi trendiksi puhua tietoturvan sijaan aina kyberturvallisuudesta. Tämä käy ilmi erinäisistä kirjallisuuslähteistä, raporteista ja artikkeleista, joita on julkaistu lähiaikoina.

Tietoturvayhtiö Kaspersky Lab on määritellyt kyberturvallisuuden olevan käytäntö, jonka avulla pyritään suojaamaan tietokoneita, palvelimia, mobiililaitteita, elektronisia järjestelmiä, verkkoja ja tietoa haitallisilta hyökkäyksiltä. Samasta asiasta voidaan vaihtoehtoisesti puhua myös termeillä informaatioteknologian turvallisuus tai sähköisen informaation turvallisuus. (Kaspersky Lab 2017)

Kyberturvallisuus käsite on yleisesti käytössä monilla eri toimialoilla ja se on jaoteltavissa useaan yleiseen luokkaan. Verkkoturvallisuus kuvaa käytäntöjä, joilla suojataan tietoverkkoja tunkeilijoilta. Sovellusturva liittyy ohjelmistojen ja laitteiden turvallisuuteen ja pyrkii suojaamaan näitä erilaisilta uhkilta, koska suojaamattomia sovelluksia voidaan käyttää pääsynä tallennettuihin tietoihin. Onnistuneeseen kyberturvallisuuteen kuuluu oleellisena osana, että nämä edeltävät mainitut asiat tulee ottaa huomioon jo suunnitteluvaiheessa, ennen minkään ohjelman tai laitteiston käyttöönottovaihetta. Tietoturva (englanniksi information security) on tarkoitettu suojaamaan tietojen eheyttä ja yksityisyyttä aina tietoa tallennettaessa, sekä tietoa siirrettäessä. Operatiivinen turvallisuus pitää sisällään prosessit ja päätökset tietovarantojen käsittelyä ja suojausta koskien. Operatiiviseen tietoturvaan kuuluu myös käyttäjien oikeuksien hallinta, eli tieto siitä, mitä ja missä tietoa voidaan tallentaa ja jakaa, kun he käyttävät verkkoa. Hätätilasta palautuminen ja yritystoiminnan jatkuvuus pitävät sisällään käytännöt, kuinka organisaatio reagoi kyberturvallisuushäiriöön tai vastaavaan tapahtumaan, joka johtaa tietojen tai toimintojen menettämiseen. Hätätilanteista palautumisen käytännöt määrittelevät, kuinka organisaatio palauttaa toimintansa ja menetetyt tiedot, sekä palaa normaalille toimintakapasiteetilleen. Liiketoiminnan jatkuvuuden käytännöt ja suunnitelma määrittävät, kuinka organisaatio toimii tilanteessa, jossa jotain tiettyjä resursseja ei ole saatavilla poikkeustilan takia. Viimeisenä osana kyberturvalli-

suuskokonaisuuteen kuuluu loppukäyttäjien koulutus, joka pitää sisällään hyvien tietoturvakäytäntöjen noudattamisen opettamisen loppukäyttäjille, mikä minimoi inhimillisistä syistä johtuvia riskejä organisaatiossa. (Kaspersky Lab 2017)

## 2.2 Esineiden Internet

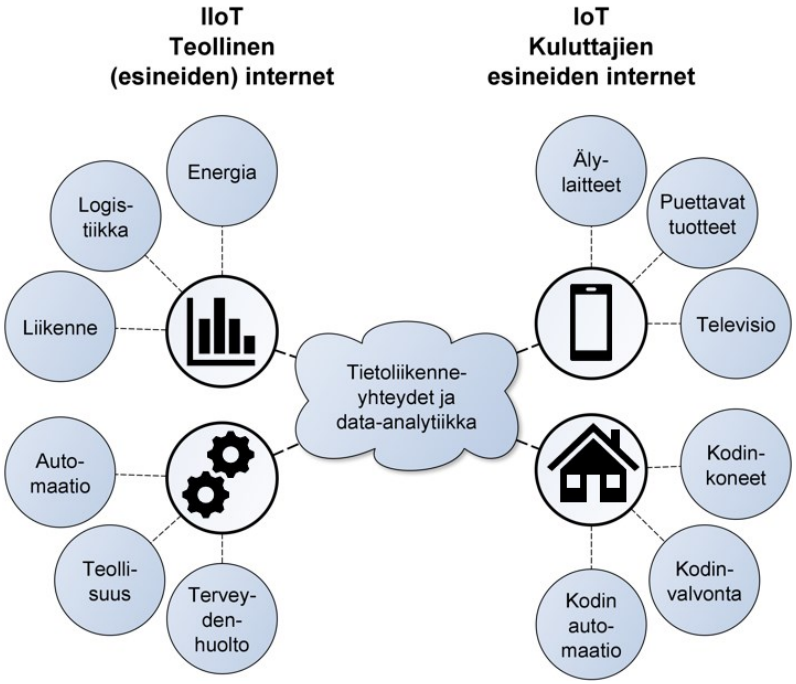
Internet of things, eli lyhyesti IoT, on suomennettuna esineiden internet. Tällä termillä viitataan heterogeeniseen joukkoon erinäisiä laitteita ja asioita, jotka on liitetty internetiin. Yhteinen piirre näillä kaikilla erilaisilla laitteilla ja asioilla on, että ne välittävät jatkuvasti itsestään verkkoon dataa. Kerätty data yleensä tallennettaan pilveen, jossa sitä voidaan analysoida. Periaatteessa voidaan todeta esineiden internetin olevan ylätason käsite, johon kuuluu osa-alueena teollinen esineiden internet, eli industrial internet of things (IIoT). Suomessa usein puhutaan vain teollisesta internetistä, vaikka tarkoitettaisiinkin teollista esineiden internetiä, vastaavasti taas IIoT-termi on käsitteenä enemmän käytössä anglo-amerikkalaisessa maailmassa. (Collin & Saarelainen 2016, Luku 2)

> Esineiden internet (IoT): globaali infrastruktuuri tietoyhteiskunnalle, joka tarjoaa edistyneitä palveluja yhdistämällä (fyysisiä ja virtuaalisia) asioita olemassa olevien ja kehittyvien yhteentoimivien tieto- ja viestintätekniikoiden perusteella. Huomautus 1 - IoT hyödyntää tunnistamisen, datan keräyksen, käsittelyn ja viestinnän ominaisuuksia hyödyntämällä kaikkia asioita tarjotakseen palveluja kaikenlaisille sovelluksille varmistaen samalla, että turvallisuus- ja tietosuojavaatimukset täyttyvät. Huomautus 2 - IoT voidaan laajemmasta näkökulmasta nähdä visiona, jolla on teknisiä ja yhteiskunnallisia vaikutuksia. (International Telecommunication Union (ITU) 2012, 1)

Käsitteenä teollinen internet mielletään yleensä tarkoittamaan vain teollisuuden käytössä olevaa internetiä, mutta tämä on hieman harhaan johtava ajattelutapa. Asiaa ei helpota lainkaan, että muun muassa Saksassa aiheesta puhutaan usein nimikkeellä Industrie 4.0 eli Teollisuus 4.0. Tähän varsinkin Saksassa käytettyyn käsitteeseen liittyy teollisen internetin käyttö juuri valmistavassa teollisuudessa. Todellisuudessa teollista internetiä hyödynnetään paljon muuallakin kuin vain valmistavassa teollisuudessa, sen yhtenä yleisenä piirteenä on kuitenkin älyn siirtyminen teollisesti valmistettaviin koneisiin ja laitteisiin. (Collin & Saarelainen 2016, Luku 2)

> Teollinen Internet on esineiden, koneiden, tietokoneiden ja ihmisten internet, joka mahdollistaa älykkään teollisen toiminnan kehittyneiden data-analytiikkojen avulla liiketoiminnan muutostuloksiin. Se ilmentää maailmanlaajuisen teollisen ekosysteemin lähentymistä, edistynyttä tietojenkäsittelyä ja valmistusta, laajamittaista tunnistamista ja kaikkialla esiintyvää verkkoyhteyttä. (Industrial Internet Consortium 2015, 8)

Esineiden internet voidaan periaatteessa jakaa kahteen osaan: teolliseen maailmaan ja kuluttajien maailmaan (Kuva 1). Näiden kahden yhdistävänä tekijänä toimivat tietoverkot ja analytiikka. Teolliseen internetiin luetaan myös mukaan julkinen infrastruktuuri ja siihen kuuluvat eri osa-alueet (Collin & Saarelainen 2016, Luku 2).




Kuva 1. Esineiden internetin jakautuminen (mukaillen Collin & Saarelainen 2016, Luku 2)

Internet of Everything eli lyhenteenä IoE ja suomeksi kaiken internet, on markkinatutkimusyhtiö Gartnerin luoma käsite, jolla pyritään kuvaamaan koko aihepiiriä mahdollisimman kattavasti. Tätä näkemystä kannattaa aktiivisesti muun muassa verkkoyhtiö Cisco. Tämä on vain yksi käytössä oleva kilpaileva käsite IoT ja IIoT käsitteiden rinnalla. (Collin & Saarelainen 2016, Luku 2)

> Internet of Things (Esineiden Internet, teollinen Internet) on toisiinsa kytkettyjen tunnistettavissa olevien fyysisten laitteiden ja esineiden muodostama verkko. (Valtioneuvoston Selvitys- ja Tutkimustoiminta 2018, 2)

Esineiden internet on laaja kokonaisuus, joka koostuu useista eri komponenteista, luoden näin erittäin heterogeenisen kokonaisuuden. Tässä opinnäytetyössä käytetään pääpainotteisesti tuota ylätason käsitettä esineiden internet eli IoT. Kyseessä on kuitenkin sama tarkasteltava ilmiö ja aihepiiri, joten myös muita termejä käytetään asiayhteydestä riippuen.

## 2.3 Pk-yritys

Pk-yritys on yleisesti käytössä oleva käsite, joka kattaa tilastokeskuksen määritelmän mukaan ne pienet ja keskisuuret yritykset, joissa on vähemmän kuin 250 työntekijää ja vuosivaihto on enintään 50 miljoonaa euroa. Taseen loppusumma ei myöskään tämän määritteen mukaa saa olla yli 43 miljoonaa euroa vuodessa. Määritelmän mukaan pk-yrityksistä ei voida puhua siinä tapauksessa, jos sen osakkeista 25 prosenttia tai sitä enemmän on jonkin toisen yrityksen omistuksessa, joka ei sovi pienyrityksen tai pk-yrityksen määritelmään. (Tilastokeskus 2020)

Ennen vuotta 2003 tilastokeskus määritteli pk-yrityksen varallisuusmääritteen alemmaksi. Tuolloin käytettiin vielä 40 miljoonan euron vuosiliikevaihtorajaa, sekä taseen loppusummasta enintään 27 miljoonan euron rajaa. (Tilastokeskus 2020)

Euroopan komissio on myös antanut oman määritelmänsä pk-yrityksistä. Se on samassa linjassa Suomen tilastokeskuksen määritelmän kanssa. Euroopan Unionin julkaisutoimiston (2020, 3–4) tuottaman julkaisun Käyttöopas pk-yrityksen määritelmä mukaan, huomioitavaa on se, että Euroopan talouden kannalta katsottuna pk-yritykset ovat erittäin tärkeässä asemassa ja muodostavat sen taloudellisen selkärangan. Euroopan Unionin ilmoittaman tilastotiedon mukaan yhdeksän kymmenestä yrityksestä EU-alueella ovat pk-yrityksiä.

Suomen Yrittäjät, Finnvera Oyj, työ- ja elinkeinoministeriö (2020, 9), julkaiseman tiedon mukaan suomessa pk-yritysten osuus kansantaloudessa on huomattava. Niiden osuus kaikista Suomen yrityksistä oli peräti 99,8 prosenttia vuonna 2018. Suomessa toimivista pk-yrityksistä 93 prosenttia on alle kymmenen henkilöä työllistäviä mikroyrityksiä. (Suomen Yrittäjät, Finnvera Oyj, työ- ja elinkeinoministeriö 2020, 9)

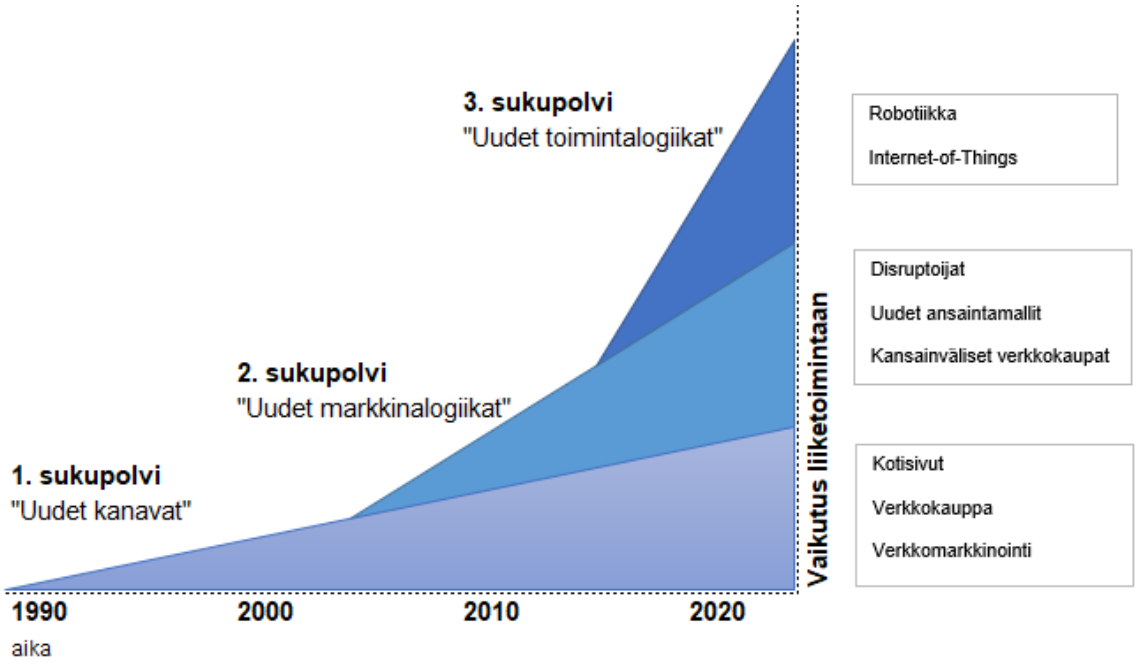
Tämän opinnäytetyön aihepiirin kannalta on huomioon otettava asia, että pk-yrityksillä on huomattavasti vähemmän henkilöstöresursseja ja varallisuutta toimia, kun niitä verrataan suurempiin yrityksiin. Nämä rajatut resurssit tarkoittavat käytännössä sitä, että kaikki raskaat ja kalliit ratkaisut eivät ole kyseisen mittaluokan yrityksille suositeltavia tai edes mahdollisia toteuttaa itsenäisesti. Tästä on mahdollista päätellä, että pk-yritysten on mahdollisesti ulkoistettava tiettyjä palveluita ja toimintoja kolmansille osapuolille ja tämä vaikuttaa myös olennaisesti tietoturvaan.

## 2.4 Digitalisaatio ja esineiden internet

Digitalisaatio on erittäin käytetty termi, mutta sille ei ole suoraa yhtenäistä virallista määritelmää. On kuitenkin tärkeä ymmärtää, että käsite pitää sisällään ajatuksen, että jokin analoginen ilmiö muunnetaan digitaaliseksi ilmiöksi, jolloin puhutaan digitalisoitumisesta. Pelkkä digitalisoituminen ei kuitenkaan ole sama asia kuin digitalisaatio. Digitalisaatiosta aletaan puhua vasta silloin, kun digitalisointi saavuttaa pisteen, jossa se muuttaa ihmisten käyttäytymistä tai markkinoita ratkaisevasti uuteen suuntaan. Tämä laaja prosessi voi myös vaikuttaa yrityksissä sen koko toimintaan ja kilpailukykyyn. Puhutaan siis tietyn tasoisesta ja laajuisesta muutoksesta, jonka digitaalinen teknologia on mahdollistanut uusien toimintamuotojen ja -tapojen kautta. (Ilmarinen & Koskela 2015, luku 2.1)

On todettava, että isojen muutosten keskellä on pk-yritysten etu pyrkiä mukautumaan uuteen tilanteeseen ja hyödyntämään uusia teknologioita täyden tuotantopotentiaalin ja paremman markkina-aseman saavuttamiseksi. Uudet teknologiset digitaalisuuteen perustuvat ratkaisut voivat tuoda kustannussäästöjä tai tehokkuutta yritysympäristöissä, joissa resurssit ovat rajallisia. Nämä teknologiat voivat myös tuoda pk-yrityksille erilaisia etuja verrattuna muihin kilpailijoihin, näiden koosta ja entisestä markkina-asemasta riippumatta. Tietoturvaa ei saisi missään nimessä unohtaa, vaan se pitää tuoda vahvasti osaksi toteutettavaa muutosta. On oletettavissa, että näin toimimalla voidaan minimoida uusien ratkaisujen mukana tulevia riskejä.

Digitalisaation eteneminen Suomessa voidaan havainnollistaa yksinkertaistetulla tavalla, ymmärtämällä siihen liittyvät tekijät ja vaiheet sukupolvina (Kuva 2). Nämä Sukupolvet eivät rajaa toisiaan pois, vaan liittyvät toisiinsa ja rakentuvat aikaisemman tason päälle. (Ilmarinen & Koskela 2015, luku 2.2)




Kuva 2. Digitalisaation kehityskulku (mukaillen Ilmarinen & Koskela 2015, luku 2.2)

Digitalisaation ensimmäinen sukupolvi toi vahvasti mukanaan uudet kanavat, eli kotisivut ja verkkokaupat, sekä erinäiset portaalit, joiden kautta mainostajat ja media saivat jalansijaa internetissä. Koska digitalisaation sukupolvet eivät ole toisiaan poissulkevia, jatkuu verkkokaupan voittokulku Suomessa edelleenkin. Toinen digitalisaation sukupolvi on ensimmäisen sukupolven jatkumo, joka toi mukanaan myös mobiili-internetin ja digitaalisuuden laajentumisen. Verkkokauppojen kehittymisen myötä globaali kilpailu on alkanut muuttaa markkinoita, joten suomalaiset yritykset joutuvat kilpailemaan ulkomaalaisten yritysten kanssa. Digitalisaatio on alkanut vaikuttamaan markkinoihin sekä luonut uusia ansaintamalleja ja lisännyt kansainvälistä kilpailua. Kolmas sukupolvi toi mukanaan muuttuneen arvontuotannon, johon vaikuttaa älylaitteiden lisääntyminen ja niiden kyky kommunikoida keskenään. Lisääntynyt automaatio ja robotiikka ovat mukana tässä murroksessa. Digitalisaation osana esineiden internet (IoT) on aiheuttanut suurta mielenkiintoa, sillä se tuo uusia mahdollisuuksia mukanaan. Tämän teknologian on odotettu muokkaavan eri toimialoja ja niiden toimintaa ratkaisevasti. Keskeisimpänä muutosvoimana on mobiiliyhteydet ja kosketusnäytölliset älypuhelimet, jotka ovat nostaneet paikkaan sitoutumattomuuden erittäin ajankohtaiseksi kokonaisuudeksi. (Ilmarinen & Koskela 2015, luku 2.2)

Digitalisaation eteneminen näkyy vahvasti digitaalisuudessa useissa uusissa laitteissa ja tavaroissa, sekä muilla osa-alueilla anturi- ja sensoriteknologioiden kehittyessä entistä älykkäämmiksi. Teollisuudessa älykkäiden anturien tuominen osaksi kaikkia laitteistoja tai niitä koskevia palveluita on osa tätä kehitystä. Tästä ilmiöstä puhutaan yleensä teollisena internetinä (industrial internet), esineiden internetinä (IoT, internet of things) tai vaihtoehtoisesti kaiken internetinä (internet of everything). (Ilmarinen & Koskela 2015, luku 4.2)

Voidaan havaita esineiden internet olevan digitalisaation luontainen jatke ja se hyödyntää aikaisempien sukupolvien mukanaan tuomia ratkaisuja. Se vie myös samalla kehitystä eteenpäin, tuomalla älykkyyttä mukaan eri ratkaisuihin. Sen avulla voidaan tavoitella lisäarvoa markkinoilla ja yhteiskunnallisessa mielessä, joka vaikuttaa myös asiakaskäyttäytymiseen. Esineiden internet on yrityksille ja yhteiskunnallisille toimijoille tästä syystä paljon mielenkiintoa herättävä kokonaisuus, joka on vielä kehittyvä teknologia. Sen käyttöönotto on vielä kesken, eikä se ole saavuttanut vielä kypsyyttä aikaisempien sukupolvien tavoin. Tästä voidaan karkeasti päätellä, että siihen liittyvät tietoturvaan vaikuttavat tekijät ovat myös kehitysvaiheessa ja kaikkia tähän liittyviä tekijöitä ei vielä tunneta tarpeeksi laajasti. Teoriassa on kuitenkin mahdollista ottaa oppia aikaisempien digitalisaation sukupolvien aikana opitusta ja soveltaa tätä tietoa pohjana uusien tietoturvaratkaisujen kehittämiseen.

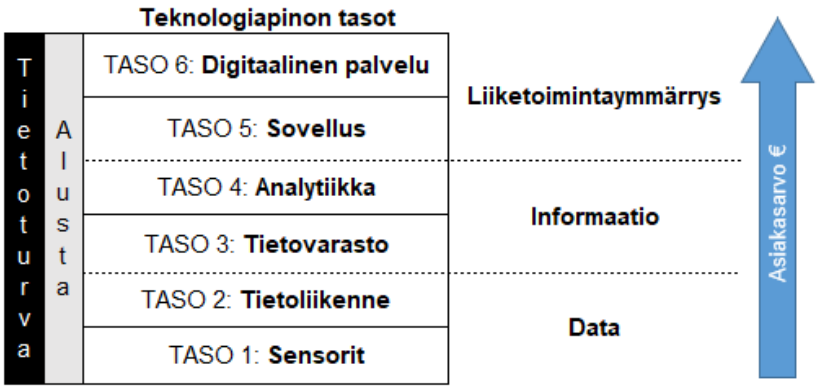
# 3 IoT-järjestelmät

Tässä luvussa kuvaillaan tyypillisen IoT-järjestelmän rakennetta sekä siihen kuuluvia ja liittyviä teknologioita, joiden päälle tai rinnalle itse järjestelmä luodaan. Luvussa pyritään tuomaan esille myös eri osa-alueisiin liittyvät tietoturvaan vaikuttavat seikat. Tämä luku on osa tietoperustaa. Siinä esitetään myös yleisiä havaintoja ja huomioita sekä johtopäätöksiä lähdemateriaalien pohjalta.

## 3.1 IoT-järjestelmän infrastruktuuri

Mitään valmista esineiden internetin pakettia ei ole vielä olemassa, joka sopisi kaikkiin mahdollisiin yritysten käyttötarkoituksiin. Tämä tarkoittaa, että yritykset joutuvat soveltamaan ratkaisuihinsa aina kulloinkin tarjolla olevaa teknologiaa, jonka avulla eri osista voidaan rakentaa yrityksen omiin tarkoituksiin sopiva infrastruktuuri. Teknologiaa on kuitenkin mahdollista ostaa palveluina alan eri toimijoilta, joka tekee alkuinvestoinneista kustannustehokkaampia, mutta ei välttämättä sido yritystä pitkällä aikajänteellä. Kyseiset ratkaisut voivat olla hyvinkin laajoja ja skaalautuvia kokonaisuuksia, jotka palvelevat liiketoimintaa tehokkaasti. (Collin & Saarelainen 2016, Luku 8)

Infrastruktuuria voidaan kuvata monessa muodossa, joista yksi suosituimmista malleista on teknologiapino. Teknologiapinossa esitetään tekniset osakokonaisuudet, joista ratkaisu koostuu (Collin & Saarelainen 2016, Luku 8). Oheisessa kuvassa 3 on esitetty kuusitasoinen versio teknologiapinosta, jota voidaan soveltaa teollisen esineiden internetin kanssa.




Kuva 3. Teknologiapino alhaalta ylöspäin (mukaillen Collin & Saarelainen 2016, Luku 8)

Teknologiapinon ensimmäiseen tasoon kuuluvat sensorit, jotka tuottavat infrastruktuurissa mittausdataa. Nämä sensorit voivat olla asennettuna esimerkiksi koneisiin, laitteisiin tai muuhun kalustoon yrityksen omien tarpeiden mukaisesti. Toisella tasolla sensoridata siirretään tietoliikenneväyliä soveltaen eteenpäin. Tietoliikenne toimii kahteen suuntaan, mikä mahdollistaa etähallinnan ja etäpäivitykset. Tähän tasoon kuuluvat verkkolaitteiden ja

verkkoteknologioiden ohella myös tietoliikenteen eri standardit ja protokollat, joita hyödynnetään tietojen välityksessä. Neljä ylempää tasoa hyödyntävät alempien tasojen tuottamaa dataa, josta jalostetaan informaatiota palvelemaan organisaation liiketoimintaa. Kolmannen tason tietovarasto on yleensä keskitetty ratkaisu, johon dataa tallennetaan. Tyypillisesti tämä tapahtuu pilvessä, koska on tarpeellista kyetä yhdistelemään dataa, joka ei ole peräisin sensoreilta, vaan kokonaan muista tietolähteistä. Muina tietolähteitä voivat olla esimerkiksi erilaiset toiminnanohjausjärjestelmät, asiakkuudenhallintajärjestelmät, yrityskumppaneiden käyttämät järjestelmät tai avoin julkishallinnon tuottama data ulkoisesta lähteestä. Neljännellä tasolla tätä yhdisteltyä datamassaa käsitellään mahdollisesti hyödyntäen pilvilaskentaa ja muita välineitä, jotka kykenevät analysoimaan massadataa. Viidennellä tasolla data siirretään sovelluksiin, jotka voivat toimia tietokone- tai mobiiliympäristössä. Tämän lisäksi dataa voidaan esittää erilaisten graafisten esitysten ja visuaalisten mittarien sekä käyttöliittymien avulla sovellusten käyttäjille. Kuudes taso on älykäs, digitaalinen lisäarvoa tuottava palvelu, joka yhdistyy organisaation liiketoimintaprosesseihin ja toimii uusien liiketoimintamallien mahdollistajana. Se yhdistää asiakkaat, toimittajat ja muut avainkumppanit kyseisiin uusiin liiketoimintaprosesseihin ja liiketoimintamalleihin. (Collin & Saarelainen 2016, Luku 8)

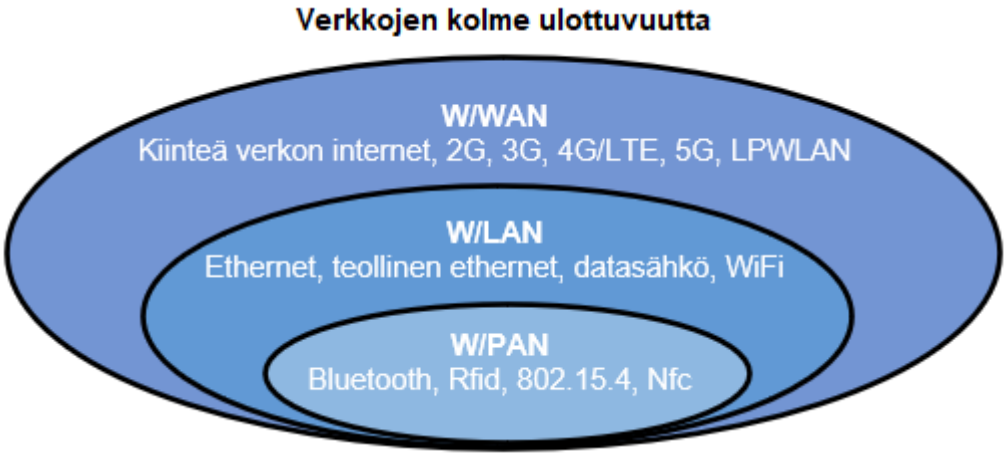
Koko teknologiapinon täytyy olla hallittavissa oleva kokonaisuus, joten kaikki tasot tuodaan yhteen käyttämällä tähän tarkoitettua alustaa. Alusta mahdollistaa hallinnan ja teknologisen yhteensopivuuden sekä huolehtii sensoreiden tuottaman datan keskitetystä keräämisestä tietovarastoon. Alusta myös tarjoaa analytiikan ja sovelluskehityksen työkalut. Tietoturva vaikuttaa koko teknologiapinoon, joten se pitää suunnitella jokaiselle tasolle sopivaksi heti alusta alkaen. Myös itse alustaan kohdistuva tietoturva on syytä suunnitella tarkasti. Vastaavan teknologiapinon rakentaminen yleensä tuottaa investointeja yritykselle, mutta yleensä se rakennetaan jo olemassa olevien IT-järjestelmien rinnalle tai mahdollisesti niiden päälle. Teknologiapino sisältää useita datalähteitä ja niiden integraation tietovarantoihin tulisi olla mahdollisimman reaaliaikaista. (Collin & Saarelainen 2016, Luku 8)

IoT-järjestelmissä käytettyjen sensorien määrä on kasvanut räjähdysmäisesti samalla, kun kustannukset ovat laskeneet. Koska anturien määrä on nykyään suuri, on niiden tuottama datamäärä myös erittäin suuri. Eräänä kehityksen suuntauksena on tällä hetkellä, että älyä yritetään lisätä suoraan sensoreihin ja ohjelmistoja siirtää ajettavaksi pilvipohjaisesti. Tämä kehitys mahdollistaa paremman etähallittavuuden ja tekee ratkaisuista päivitettäviä, jolloin suurin osa ylläpidosta voidaan toteuttaa pilvialustan kautta etähallinnan avulla. Tietoliikenteen määrää pyritään pitämään järkevissä rajoissa viemällä prosessointia mahdollisimman lähelle sensoria. Tämä käytännössä tarkoittaa sitä, että pilveen pyritään ajamaan

vain helposti hyödynnettävässä muodossa olevaa dataa. Nykyään on myös alettu käyttämään langattomia sensoreita ja tiedonsiirtoa hyödyntäen esimerkiksi eri mobiiliverkkoja. Langattomien anturien käytön uskotaan lisääntyvän jatkossa erittäin paljon. (Collin & Saarelainen 2016, Luku 9)

Tietoliikenteen toteuttamiseen on olemassa lukuisia eri vaihtoehtoisia verkkoteknologioita, menetelmiä, standardeja ja protokollia. Kaikissa vaihtoehdoissa on kuitenkin erilainen kantama, tietoliikenteen nopeus, virrankulutus ja mahdollisesti verkon topologia sekä eroja tietoturvassa. Protokollat ja standardit muodostavat erittäin tärkeän kokonaisuuden tietoliikenteessä, mutta käytettyjen protokollien tietoturvaerot vaikuttavat suojausperiaatteesta lähtien aina suojauksen vahvuuteen asti. Tietoturvan kannalta paras mahdollinen tilanne on pyrkiä supistamaan käytössä olevien verkkoteknologioiden määrä mahdollisimman pieneen, mutta käytännössä tätä on hankala toteuttaa. Yritysympäristössä saattaa olla tietoliikenne teknologioita käytössä, joiden päälle uudet ratkaisut voidaan rakentaa. Vaarana aikaisemmissa ratkaisuissa on, että kyseinen teknologia voi olla vanhanaikaista tai ei sovellu kunnolla uuteen tarkoitukseen. Yhteensopivuus, päivitettävyys ja toimivuus voivat nousta tuolloin myös ongelmiksi. Ennusteena on, että langattomien ratkaisuiden määrä tulee kasvamaan huomattavasti, mutta vielä monessa tilanteessa pyritään hyödyntämään langallista verkkoa. Langattoman verkon etuna on, että sitä on huomattavasti helpompaa ja nopeampaa laajentaa tarpeiden mukaan. (Collin & Saarelainen 2016, Luku 10)

Langallisten ja langattomien verkkojen kattavuus voidaan jakaa kolmeen ulottuvuuteen, jotka ovat tyypillisesti langallisen verkon kohdalla PAN, LAN ja WAN tai langattomien verkkojen kohdalla WPAN, WLAN ja WWAN (Kuva 4). Näiden eri ulottuvuuksien kanssa hyödynnettävät teknologiat ja protokollat voivat vaihdella suurestikin. (Collin & Saarelainen 2016, Luku 10)




Kuva 4. Verkkojen kolme ulottuvuutta (mukaillen Collin & Saarelainen 2016, Luku 10)

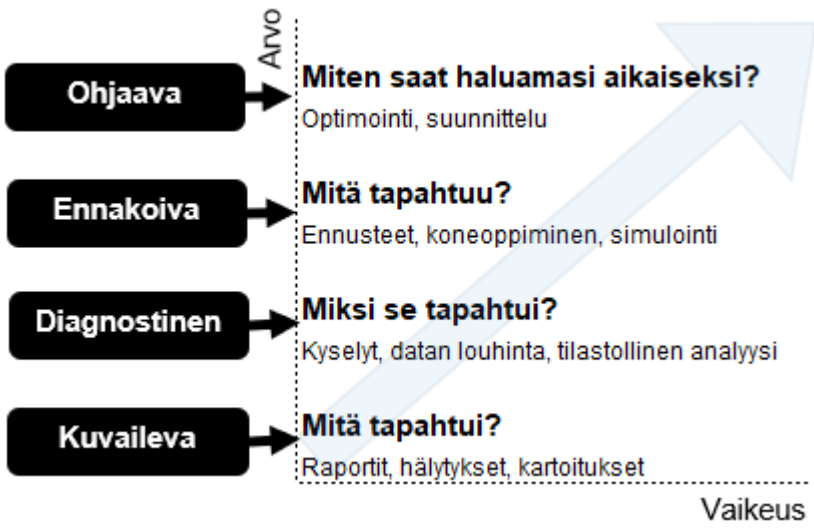
Eri verkkotyyppien ominaisuudet, kantamat ja tiedonsiirtokapasiteetti vaihtelevat huomattavasti, sillä ne on kaikki tarkoitettu erilaisiin skenaarioihin palvelemaan jotain tiettyä tarkoitusta. Perinteisesti verkot ovat pitkään olleet lähtökohtaisesti langallisia, jotka tietoturvan ja toimintavarmuuden takia on yleensä jaettu aliverkkoihin. Tämä on tyypillisesti toteutettu kytkimiä käyttäen ja verkko on voitu vielä eristää esimerkiksi muusta toimiston intranetistä palomuureilla. Tällä hetkellä ongelmallista verkon suunnittelun kannalta on se, että standardoinnissa on havaittavissa puutteita. Tämä aiheuttaa fragmentoitumista ja eri toimittajien suosimat suljetut ratkaisut eivät auta asiaa. Ongelmia voi periytyä myös aikaisemmin käyttöön otetuista laitteistoista tai automaatioväylistä ja muista vanhoista käytössä olevista komponenteista. (Collin & Saarelainen 2016, Luku 10)

Teknologiapinon kolmannen tason tietovaraston tyyppinä hyödynnetään yleensä SQL- tai NoSQL-tietokantaa. Tietovarasto voidaan arkkitehtuurisesti toteuttaa keskitetysti tai hajautetusti ja siihen liittyvät integraatiot on myös mahdollista toteuttaa monella eri tavalla. Valitun ratkaisun skaalautuvuus on tärkeää, koska datan määrä kasvaa jatkuvasti, vaikka dataa voidaankin tiivistää tietovarastossa tilan säästämiseksi erilaisten algoritmien avulla. NoSQL:n suosio on jatkuvassa nousussa, johtuen sen merkittävästä roolista massadatan ja teollisen internetin kanssa. Se tarjoaa hyvän suorituskyvyn ja joustavuuden, mutta tiedon eheyden varmistaminen ei lukeudu sen vahvuuksiin. Tästä johtuvat riskit ovat kuitenkin yleensä muilla keinoilla hallittavissa. Tietoverkon keskitetty arkkitehtuuri on yleensä varsin riittävä ratkaisu, mutta tietyn pisteen jälkeen varsinkin autonomisten ja älykkäiden laitteiden kohdalla on parempi käyttää hajautettua arkkitehtuuria, koska hajautettu ratkaisu mahdollistaa muun muassa P2P-vertaisviestinnän laitteiden välillä. Hajautettu järjestelmä mahdollistaa myös hajautetun auditoinnin ja hajautetun datan jakamisen, mutta tietoturvan kannalta kyseinen ratkaisu vaatii luotettujen yhteyksien luomista ja ylläpitämistä. Nämä tietoturvaan liittyvät toiminnallisuudet on syytä automatisoida mahdollisimman pitkälle, ja yksi uudemmista ratkaisuista tähän on lohkoketjuteknologian soveltaminen. (Collin & Saarelainen 2016, Luku 11)

Neljännellä teknologiapinon tasolla tapahtuva analytiikka mahdollistaa osaltaan paremman päätöksenteon, tilanteiden ennakoimisen ja toiminnan tehostumisen. Analytiikan avulla datasta pyritään esittämään informaatiota, joka auttaa ratkaisemaan liiketoiminnan kannalta kriittisiä kysymyksiä. Analytiikassa pyritään käyttämään tehokkaita algoritmeja automatisoimaan datan tulkintaa, mikä vapauttaa resursseja ja vähentää manuaalista työtä. Näitä algoritmeja voidaan ajaa teknologiapinon eri tasoissa yhden ison tietojärjestelmän sijasta. Tarjolla on olemassa monia valmiita pilvipalveluita, jotka soveltavat tekoälyä analytiikassa. Suurista ja merkittävistä palveluntarjoajista sekä palveluista mainittakoon IBM Watson IoT-alusta, Microsoft Azure-pilvipalvelu, Amazon AWS-pilvipalvelu ja

Googlen Coud-alusta. Analytiikassa käytetään varsinkin massadatan louhimisen yhteydessä koneoppimisen lisäksi neuroverkkolaskentaa ja muita tekoälyyn, tilastotieteeseen ja matematiikkaan nojautuvia menetelmiä. Tekoäly voi oppia suoriutumaan eri tehtävistä, mutta se vaatii koulutusta, johon hyödynnetään kerättyä dataa. Tekoälyllä on kolme eri oppimismenetelmää: ohjattu oppiminen, vahvistusoppiminen ja ohjaamaton oppiminen, joista viimeisin on myös vaativin toteutettava malli. (Collin & Saarelainen 2016, Luku 12)

Analytiikassa on neljä eri tasoa: kuvaileva, diagnostinen, ennakoiva ja ohjaava. Jokainen näistä tasoista pyrkii vastaamaan eri kysymyksiin. Analytiikan avulla saavutettavan arvon kasvaessa myös toteutetun analytiikan vaikeusaste kasvaa (Kuva 5).



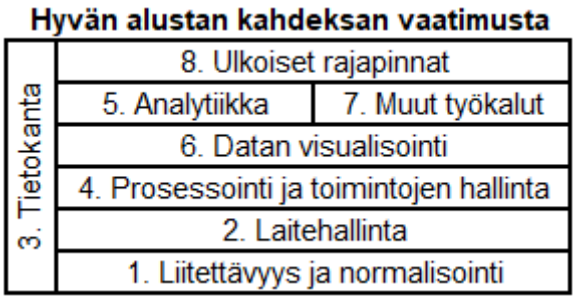

Kuva 5. Analytiikan tasot (mukaillen Collin & Saarelainen 2016, Luku 12)

Teknologiapinon viidennen tason eli sovelluksen luominen on mahdollista ulkoistaa, mutta silloin täytyy tietää, mitä oikeuksia dataan voidaan antaa sovelluskehittäjille, ja mitkä muut tiedot ovat tarpeellisia sovellusta suunniteltaessa ja rakennettaessa. Sovellustaso on yhteydessä teknologiapinon alempiin tasoihin, mikä tapahtuu sovelluskehityksessä API:n (application programming interface), eli rajapinnan avulla. Teknologiapinoon valittu IoT-alusta määrittelee sovelluskehitystä hyvin pitkälle. Tämä johtuu siitä, että suurin osa alustoista tukee suoraan REST-rajapintaa, mutta muitakin vaihtoehtoja on saatavilla. Sovellus yleensä luodaan käyttämällä ketterän kehityksen suuntauksia, jolloin se on myös hyvä pitää helposti muokattavissa ja laajennettavissa tarpeen mukaan. Iso osa moderneista sovelluksista toimii SaaS-periaatteella pilvipalveluna selaimen kautta, jolloin ohjelmisto ei ole sidottu päätelaitteen tyyppiin ja malliin. Tämä mahdollistaa mobiililaitteiden hyödyntämisen entistä helpommin ja parantaa tietoturvallisuutta, koska webbisovelluspohjaisten ratkaisujen taustajärjestelmän dataa ei tallennu päätelaitteisiin. Joskus edeltävä ei kuitenkaan ole

mahdollista ja silloin on toteutettava perinteinen järjestelmäsidonnainen sovellusratkaisu. (Collin & Saarelainen 2016, Luku 13)

Teknologiapinon kuudes taso, eli digitaalinen palvelu, yhdistää teknologiapinon yrityksen liiketoimintaan. Tällä tasolla syntyy varsinainen tuote, jota yritys voi myydä asiakkailleen. Tuote voi olla esimerkiksi ennakoiva huoltopalvelu tai vaikka jokin muu käyttökustanteinen palvelumalli. Digitaalisissa uusissa palveluissa on neljä eri tunnuspiirrettä, jotka ovat reaaliaikaisuus, ennakoitavuus, mobiliteetti ja automaatio. Palvelussa kerättävä data on siis pienellä latenssilla analysoitavissa ja muunnettavissa hyödylliseksi informaatioksi. Datasta on analytiikan ja koneoppimisen avulla mahdollista ennustaa asioita ja muutoksia. Palvelu on saatavissa päätelaiteriippumattomasti ja ei paikkaan sidotusti. Prosessiautomaation avulla on poistettu turhia manuaalisia työvaiheita ja suoraviivaistettu prosesseja. (Collin & Saarelainen 2016, Luku 14)

Teknologiapinossa alusta yhdistää aineellisen ja virtuaalisen maailman yhdeksi kokonaisuudeksi, mutta se myös yhdistää teknologiapinon tasot toisiinsa. Alusta kattaa laajalti tietoturvan ja voi sisältää myös suuren osan teknologisesta infrastruktuurista ja sen toiminnoista. IoT-alustan määritelmä on hyvin väljä, eikä sille ole olemassa mitään yleistä standardia. Alusta kuitenkin mahdollistaa IoT-päätepisteiden valvonnan ja hallinnoinnin sekä sovelluskehityksen. Alusta ei varsinaisesti ole pakollinen komponentti järjestelmässä, mutta sen puuttumisesta voi seurata hankaluuksia muun muassa teknologiapinon hallittavuudelle. Hyvä alusta täyttää kahdeksan yleistä vaatimusta: liitettävyys ja normalisointi, laitehallinta, tietokanta, prosessointi ja toimintojen hallinta, analytiikka, datan visualisointi, muut työkalut sekä ulkoiset rajapinnat (Kuva 6). Tässä yhteydessä muilla työkaluilla tarkoitetaan lähinnä kehitys-, hallinta- ja raportointityökaluja. Hallintatyökaluilla voidaan esimerkiksi rajata, kenellä on pääsy dataan tai sensoreihin, eli niillä hallinnoidaan käytännössä tietoturvaa. (Collin & Saarelainen 2016, Luku 15)




Kuva 6. Hyvän alustan vaatimukset (mukaillen Collin & Saarelainen 2016, Luku 15)

Avoimen lähdekoodin alustaratkaisut, jotka ovat itse kehitettyjä ja yrityksen itse räätälöitävissä, sisältävät tietoturvan kannalta riskin. Näissä tilanteissa tietoturvapäivitykset jäävät

yrityksen omalle vastuulle, eli tietoturvan taso on kaupalliseen ja ylläpidettyyn ratkaisuun nähden kyseenalaisempi. Kaupalliset ratkaisut aiheuttavat kustannuksia yritykselle, mutta vielä kalliimpaa on korjata jatkuvasti itse tietoturva-aukkoja jälkikäteen itse räätälöidystä ratkaisusta. Valmiit kaupalliset ratkaisut madaltavat myös yritysten kynnystä hyödyntää pilvikeskeisiä ratkaisuja. Kotimaisia kaupallisia alustaratkaisuja on tarjolla muun muassa Elisa IoT, Telia IoT, Tieto Connect, Wapice IoT-Ticket, BaseN Platform ja VTT IoT Gateway. Näiden lisäksi yrityksille on tarjolla lukemattomia ulkomaalaisia kaupallisia sekä avoimen lähdekoodin valmiita ja puolivalmiita ratkaisuja. (Collin & Saarelainen 2016, Luku 15)

### 3.2 IoT-järjestelmän tiedonsiirron periaatteet

Tiedonsiirron protokollat voidaan ryhmitellä tiedonsiirron periaatteen mukaisesti, jolloin teollisessa esineiden internetissä nousee esille kolme eri mallia. Yleisin malli näistä on niin kutsuttu julkaisija-tilaaja-malli. Analytiikan ja datan keskitetyn keräämisen kannalta julkaisuja-tilaaja-malli on selvästi hyvä ratkaisu. Tämä johtuu siitä, että julkaisija ja tilaaja ovat riippumattomia toisistaan ja ne on siksi mahdollista korvata helposti tarvittaessa esimerkiksi poikkeustilanteissa tai laitteen rikkoutumisen yhteydessä. Tässä mallissa päätepisteet ovat julkaisijan roolissa ja data julkaistaan aiheen mukaisesti. Dataa siirretään verkossa keskitetyn pisteen kautta tilaajan roolissa olevalle kohteelle. Tilaajan roolissa voi olla tietokanta, sovellus tai jokin muu päätepiste, mutta on myös mahdollista, että päätepiste voi olla järjestelmässä samaan aikaan julkaisija ja tilaaja. Toinen vaihtoehtoinen malli perustuu asiakas-palvelin-mallin kyselyihin. Palvelin siis lähettää tässä mallissa tietoa, vain siltä erikseen kysyttäessä. Verkon kuormittavuutta ajatellen tämä on kevyt ratkaisu, koska sensoridataa voidaan kerätä paikalliseen puskurimuistiin. Sitä voidaan myös suodattaa ja pakata ennen seuraavan lähetyspyynnön saapumista. Negatiivisena puolena on se, että päätelaite ei voi olla lepotilassa, koska se odottaa aina seuraavaa pyyntöä. Teoriassa on myös mahdollista, että jatkuvasti kasvavat kyselymäärät voivat olla verkkoa ruuhkauttavia, mutta vasta tietyn pisteen jälkeen. Näiden edeltävien mallien lisäksi tiedonsiirto on mahdollista toteuttaa vertaisverkko periaatteella, eli tieto vaihtuu symmetrisesti päätelaitteiden välillä. Kyseinen malli sopii tilanteisiin, joissa tiedonsiirron latenssin täytyy pysyä pienenä. (Collin & Saarelainen 2016, Luku 10)

### 3.3 IoT-yhdyskäytävät

IoT-yhdyskäytävä on laite, jolla yhdistetään eri protokollien avulla kaksi verkkoa toisiinsa, vaikka verkot eivät olisi keskenään ollenkaan samankaltaisia. IoT-yhdyskäytävän tyypillinen sovellus on reititin, joka yhdistää yksityisen verkon ja internetin. Se voi kerätä dataa ja lähettää sitä eteenpäin esimerkiksi pilvipalvelulle, mutta sen kautta on myös mahdollista siirtää tietoa molempiin suuntiin eri verkkojen ja järjestelmien välillä. IoT-yhdyskäytävät

ovat teknologiana verrattain uusi asia, mutta niiden avulla saavutettavat hyödyt vaihtelevat kulloinkin käytettävän laitteen joustavuudesta ja monipuolisuudesta riippuen, esimerkiksi fyysiset liitännät, käyttöjärjestelmät ja laitteen omat tarjolla olevat resurssit vaikuttavat tähän yhtälöön. IoT-yhdyskäytävät eivät ole pakollinen asia, mutta ne tarjoavat vaihtoehtoja ja lisäominaisuuksia perinteisten sovellusratkaisujen rinnalle. Varsinkin teollisuuskäytössä yhdyskäytävät voivat olla hyvinkin tarpeellisia välikomponentteja. (LAMKpub 2019)

Yhdyskäytäviä on saatavilla suoraan valmisratkaisuina, tai ne on myös mahdollista räätälöidä tapauskohtaisesti sopimaan toimialan ja ympäristön tarpeisiin. Jotkin tarjolla olevat ratkaisut ovat suljettuja ja suunniteltu toimimaan vain tiettyjen laitetoimittajien toimittamien omien kokonaisuuksien kanssa. Yhdyskäytävien etuihin kuuluu, että ne suodattavat raakadataa ja vähentävät näin osaltaan tietoliikenteen määrää verkossa. Ne myös suojaavat sensoreilta tuotua dataa mahdollisissa yhteysongelmatilanteissa, koska yhdyskäytävä kykenee puskuroimaan dataa omaan muistiinsa. (Collin & Saarelainen 2016, Luku 10)

### 3.4 Esineiden internet ja standardointi

IEEE-standardointijärjestö valmisteli syksyllä 2016 kaiken kattavaa esineiden internet IEEE P2413 -standardointihanketta. Kyseisen hankkeen keskeisenä tarkoituksena on määritellä arkkitehtuurikehys, joka mahdollistaa yhteensopivuuden ja datan jakamisen teollisissa järjestelmissä, kotiautomaation kanssa, liikenteessä ja muiden sovellusalueilla käytettyjen laitteiden ja sovellusten kanssa. Hankkeessa on mukana satoja eri johtavia yrityksiä eri toimialoilta. Maailmalla on myös muita kilpailevia IoT-standardointihankkeita, joissa on mukana eri yrityksiä. Nämä kilpailevat standardit on luotu palvelemaan tiettyjen IoT-sovellusalueiden tarpeita ja voivat olla hyödyllisiä omilla tahoillaan, mutta myös aiheuttaa standardien välistä ongelmaa tulevaisuudessa. (Collin & Saarelainen 2016, Luku 10)

IEEE 2413-2019, eli IEEE-standardi esineiden internetin arkkitehtuurikehykselle (IoT) on saanut standardointijärjestön hyväksynnän 21.5.2019. Se on julkaistu kokonaisuudessaan 10.3.2020. Kyseinen standardointi on erittäin kattava, ja sen arkkitehtuurinen kehys perustuu aikaisempaan IEEE P2413-vedokseen. (IEEE Standards Association (IEEE SA) 2020)

Standardointi auttaa yrityksiä ja organisaatioita luomalla yhteisiä pelisääntöjä, joiden puitteissa toimiminen takaa parhaan mahdollisen yhteensopivuuden ja tuloksellisuuden. Tietoturvan kannalta on hyvä huomioida, että kattavat standardoinnit poistavat fragmentaation tuomia ongelmia ja yksinkertaistavat ylläpidon toimenpiteitä. On oletettavaa, että menee kuitenkin aikaa ennen kuin tuoreiden standardien hyödyt konkretisoituvat näkymään varsinkin pienten toimijoiden, kuten pk-yritysten toimintaympäristöissä. Hyvien raamien

luominen on kuitenkin askel kohti oikeaa suuntaa, jolloin on oletettavissa, että tulevaisuudessa tulemme näkemään yhteensopivampia ratkaisuja, mikä omalta osaltaan varmasti vaikuttaa tietoturvasuunnitteluun positiivisesti.

### 3.5 Mobiilitiedonsiirto

Uudet viidennen sukupolven 5G-mobiiliteknologiat tekevät parhaillaan tuloaan, mutta tämän runkona toimii nykyään jo käytössä oleva paranneltu 4G-verkko. 5G mahdollistaa paremman datansiirron ja kapasiteetin, mutta se ei kuitenkaan tule korvaamaan 4G-verkkoa täysin vielä pitkään aikaan. Yksi merkittävä tekijä 5G:n kehitykseen on esineiden internet, joten se pyrkii laskemaan latenssia, nostamaan tiedonsiirtokapasiteettia ja käyttäjämäärää verkossa verrattuna aikaisempiin ratkaisuihin. Nykyisin käytössä oleviin neljännen sukupolven mobiilitiedonsiirtoratkaisuihin lukeutuvat myös teknologiat NB-IoT (Narrow Band Internet of Things) ja LTE-M, jotka on suunniteltu palvelemaan erityisesti esineiden internetin ja yritysten tarpeita. Nämä teknologiat ovat käytettävissä myös 5G:n tullessa, jolloin uudet verkkoprotokollat voivat siirtää dataa luotettavasti mobiiliverkossa. Kehitys tähtää myös siihen, että esineiden internetin yhteydessä käytettävien langattomien sensoreiden akkukestoa voidaan venyttää erittäin pitkäksi, kun käytössä ovat uudet tiedonsiirtoprotokollat ja verkkoteknologiat. (DNA Business 2020, 5–8)

Tietoturvayhtiö Kasperskyn (s.a.) mukaan 5G:n kyberturvallisuudessa on joitain huolestuttavia piirteitä. Esimerkiksi 5G-verkkojen turvallisuus on hyvin hajautettua, koska se koostuu useammasta yhteyspisteestä, joita on todennäköisesti vaikeampi valvoa aikaisempiin sukupolviin verrattuna. Kyseisessä tilanteessa suojaamaton alue voi vaarantaa koko verkkoa. Myös 5G:n mukanaan tuoma kaistanleveys saattaa tehdä siitä palveluntarjoajalle hankalampaa valvoa tosiaikaisesti, joten haasteena on luoda uusia menetelmiä kattamaan valvonnan tarpeet. Esineiden internetin kohdalla ongelmaksi nousee tietoturvastandardien puutteet, minkä vuoksi verkkomurrot ja hakkeroinnit ovat yleistymässä varsinkin halpojen laitteiden kohdalla, koska niiden tietoturva ei ole prioriteetti valmistajille. IoT-laitteiden valtava määrä myös nostaa mahdollisten murtopisteiden määrää huomattavasti. 5G-verkossa on myös salauksen kannalta puute yhteydenmuodostuksen alkuvaiheessa, mikä mahdollistaa esineiden internetin laitteisiin kohdennetut hyökkäykset. Kasperskyn ilmoittamien tietojen mukaan tietoturva-aukkojen takia on muun muassa mahdollista suorittaa bottiverkkohyökkäyksiä, palvelunestohyökkäyksiä (DDoS) ja väliintulohyökkäyksiä (MiTM) sekä toteuttaa sijainnin seurantaa ja puhelunsieppauksia. (Kaspersky Lab s.a.)

Huomioitavaa on, että esineiden internet ja samalla siihen liittyvä mobiliteetti on vielä edelleen kehittyvä kokonaisuus. Samaa voidaan sanoa mobiiliyhteyksistäkin, joita esineiden internetin kanssa on mahdollista soveltaa. Markkinoilla on 4G- ja 5G-yhteyksien lisäksi

paljon muitakin vaihtoehtoja, joissa kaikissa on aina omat vahvuutensa ja heikkoutensa. Uusien käytettävien teknologioiden mahdollisuudet ja riskit on joka tapauksessa hyvä tiedostaa ja kartoittaa jo ennen niiden varsinaista käyttöönottoa.

### 3.6 Reunalaskenta

Reunalaskenta (englanniksi edge computing) on teknologiasuuntaus, jonka oletetaan nousevan suureksi IT-trendiksi tulevaisuudessa. Termi on jokseenkin vakiintunut käytössä ja sillä viitataan teknologiaan, jota hyödynnetään IoT-laitteiden keräämän datan käsittelyssä mahdollisimman lähellä datan keräyspistettä. Reunalaskennan avulla kerättyä dataa ei tarvitse välttämättä siirtää ollenkaan palvelimelle, jolloin sen prosessointi helpottuu ja nopeutuu. Tämä myös tarkoittaa sitä, että hyödynnettävään pilvipalveluun tallennettaan vain hyödyllinen prosessoitu data, joka on yritystoiminnan kannalta luokiteltu arvokkaaksi. (Telia Compan 2020)

Reunalaskentaa käytetään täydentämään tulevaisuudessa pilviteknologian etuja, varsinkin tilanteissa, joissa automatisaatiota on viety pitkälle. Kasvavana trendinä on, että yritykset ovat luopumassa omista konesaleista ja siirtämässä toiminnallisuutta pilveen. Pilviteknologia kuitenkin tuo mukanaan tiettyjä mahdollisia teknisiä ongelmia, esimerkiksi toimintakatkojen muodossa. Reunalaskennan yleistymisen uskotaan auttavan näissä tilanteissa. (Mikrobitti 2021)

Reunalaskennan tietoturvasta ei löydy vielä tähän kyseiseen aiheeseen liittyvää tietoa teoreettisia kirjoituksia lukuun ottamatta. Suurimmaksi osaksi tämä johtuu siitä, että kyseessä on varsin uusi ja kehittyvä teknologia, joten sen ympärille ei ole muodostunut vielä vahvoja yleisesti parhaaksi todettuja käytänteitä. Joitakin artikkeleita on mahdollista löytää suomeksi, jossa pohditaan, kenelle reunalaskennan tietoturvan hoitaminen todella kuuluu, mutta aihe rajoittuu tämän opinnäytetyön rajauksen ulkopuolelle. Karkeasti ottaen tilannetta hämärtää se, että tietoturvan taso ja siitä huolehtiminen riippuu kyseisen teknologian implementointimallista, eli se on hyvin tilannekohtaista. Nyrkkisääntö näyttäisi olevan, mikäli ratkaisu ostetaan operaattorilta, niin he vastaavat tietoturvasta. Mikäli reunalaskenta-ratkaisu otetaan itse yrityksen tiloissa käyttöön, niin ratkaisu on yleensä omalla tai toimittajan vastuulla.

### 3.7 Pilvipalvelut

Pilvipalvelut ovat palvelumallikokonaisuus, josta käytetään myös termiä pilvilaskenta. Nämä palvelut mahdollistavat tarpeen mukaan verkkoyhteyden yli saatavilla ja käytettävissä olevat jaetut tietokoneresurssit. Näihin jaettuihin resursseihin kuuluvat esimerkiksi,

verkot, palvelimet, tallennustila, sovellukset ja palvelut. Resursseja voidaan hallinnoida helposti ja ottaa käyttöön tarpeen mukaan. Resursseja voidaan myös vapauttaa, kun niitä ei enää tarvita. (Mell & Grace 2011, 2)

> Uudet teknologiat kuten tekoäly, IoT ja pilvipalvelut ovat muodostuneet yrityksille elintärkeiksi ja mahdollistavat täysin uusien liiketoimintojen synnyn. (Uusiteknologia 2018, 2)

Pilvilaskennalle on luokiteltu viisi keskeistä olennaista ominaisuutta, jotka ovat itsepalveluperiaate, laaja verkkosaatavuus, resurssien yhdistely, nopea joustavuus ja palvelun mitattavuus. Pilvilaskentaan on laaja pääsy verkon kautta, joten käytännössä sen ominaisuuksiin pääsee käsiksi vakiomekanismien avulla asiakasalustasta riippumatta, esimerkiksi käyttäen älypuhelinta, tablettia tai tietokonetta. Palveluille on ominaista resurssien yhdistely siten, että palveluntarjoajan resursseja voi samanaikaisesti käyttää useampi asiakas. Tällöin erilaiset fyysiset ja virtuaaliset resurssit jakaantuvat dynaamisesti asiakkaiden kysynnän mukaan. Palvelu on paikkariippumaton ja usein asiakkaalla ei ole tarkkaa tietoa toimitettujen resurssien sijainnista. Asiakkailla on kuitenkin yleensä mahdollisuus määrittää esimerkiksi tahdottu maa, osavaltio, provinssi tai datakeskus, josta resurssit dynaamisesti otetaan käyttöön. Palveluiden nopea joustavuus takaa hyvän skaalautuvuuden resurssien kysynnän mukaan. Kyseessä on mitattu palvelu ja usein laskutus toimii kulloinkin käytettyjen resurssien perusteella mittauksen mukaisesti. (Mell & Grace 2011, 2)

Pilvilaskennalle on luokiteltu kolme eri palvelumallia, jotka ovat ohjelmisto palveluna (SaaS), alusta palveluna (PaaS) ja infrastruktuuri palveluna (IaaS). SaaS-malli mahdollistaa palveluntuottajan tarjoamien applikaatioiden käytön pilvi-infrastruktuurissa. Tällaiset sovellukset usein toimivat nettiselaimen kautta, joten niihin pääsee käsiksi useilla eri laitteella. Asiakkaalla ei ole oikeuksia hallinnoimaan taustalla olevaa pilvi-infrastruktuuria, eli verkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa tai yksittäisiä ohjelmistoja. Poikkeuksena harvoissa tapauksissa tähän on käyttäjäkohtainen rajattu sovellusasetuksiin pääsy. PaaS on asiakkaille tarjottava palvelumalli, joka mahdollistaa asiakkaan itse hankkimien tai luomien applikaatioiden asentamisen ja käyttämisen pilvi-infrastruktuurissa. Asiakkaalla ei tässä mallissa ole oikeuksia hallita taustalla olevaa pilvi-infrastruktuuria, mutta hän voi hallinnoida käyttöönotettuja sovelluksia ja mahdollisesti sovellusasennusympäristön asetuksia. IaaS-malli tarjoaa asiakkaalle resurssien varauksen, tallennustilan, verkot ja muut perusresurssit, joita käytetään pilvilaskennassa. Asiakas voi asentaa, ottaa käyttöön ja suorittaa haluamiaan ohjelmistoja vapaasti. Asiakkaalla ei kuitenkaan ole oikeuksia hallinnoida taustalla toimivaa pilvi-infrastruktuuria, mutta saa kuitenkin hallinnoida va-

paasti käyttöön ottamiaan käyttöjärjestelmiä, tallennustilaa ja ohjelmistosovelluksia. Asiakkaalla voi olla myös oikeudet hallinnoida rajatun verkkoalueen komponentteja, kuten esimerkiksi isäntäpalomuureja. (Mell & Grace 2011, 2–3)


Kuva 7. Pilven monet kasvot – IaaS, PaaS ja SaaS (mukaillen Telia Inmics-Nebula Oy 2018)

Kuten kuvasta 7 voidaan havaita, palveluiden vastuualueiden jakautuminen toimittajan ja asiakkaan kesken vaikuttaa myös tietoturvaan ratkaisevasti. Palveluntarjoaja vastaa siitä vain tiettyyn pisteeseen asti, riippuen aina valitusta palvelumallista, joten muissa tapauksessa tietoturva on asiakkaan vastuulla. Organisaatioiden perinteisen mallin mukaisesti omiin toimitiloihin sijoitettavaan ratkaisuun viitataan kuvassa 7 nimikkeellä ”on premises”.

Yrityksen omien resurssien puuttuessa on erittäin järkevää ulkoistaa tietyt osa-alueet ja tukeutua palveluntarjoajan ammattitaitoon, joka vastaa myös tietoturvasta tarjottujen palveluiden osalta. Tämä tarkoittaa käytännössä sitä, että oikean palveluntarjoajan löytäminen on erittäin tärkeää. Asiasta on mahdollista tehdä kattava selvitys, jossa määritetään, täyttääkö palvelu ja palveluntarjoaja yrityksen asettamat vaatimusmääritelmät. Myös palveluntarjoajien koko ja asema markkinoilla voi luoda luotettavuutta, mutta se tuo toisaalta myös näkyvyyttä. Tätä on punnittava tietoturvan näkökulmasta aina, kun hankintoja tehdään. Mahdolliset auditoinnit kannattaa käydä läpi, jotta saadaan tarpeeksi vankka pohja edetä hankinnassa, varsinkin esineiden internetin ratkaisujen suhteen tämä voi olla hyvinkin tärkeä vaihe.

Pilvilaskennan käyttöönottomalleja on neljää erilaista: yksityinen pilvi, yhteisön pilvi, julkinen pilvi ja hybridipilvi. Yksityinen pilvi on pilvipalveluinfrastruktuuri, joka tarjotaan vain yhdelle organisaatiolle. Yritys voi omistaa palvelun, hallinnoida sitä, toimia sen ylläpitäjänä tai se voi olla kokonaan kolmannen osapuolen vastuulla. Myös näiden vaihtoehtojen yhdisteleminen on mahdollista. Kyseinen palvelu voi olla tuotettuna organisaation omissa

toimitiloissa tai niiden ulkopuolella. Yhteisön pilvi on varattu jonkin tietyn organisaatioiden muodostaman yhteisön käytettäväksi. Tällaisella yhteisöllä voi olla esimerkiksi yhteisiä tavoitteita liittyen toteutettavaan tehtävään, turvallisuusvaatimuksiin, käytäntöihin tai muiden vaatimusten noudattamiseen liittyen. Kyseisen palvelun voi omistaa tai hallinnoida yksi tai useampi yhteisöön kuuluva organisaatio, mutta myös jokin kolmas osapuoli tai näiden vaihtoehtojen yhdistelmä. Palvelu voidaan toteuttaa yhteisöön kuuluvan organisaation toimitiloissa tai sen ulkopuolella. Julkinen pilvi on järjestetty suuren yleisön avoimeen käyttöön. Se voi olla jonkin yrityksen, akateemisen tahon, julkisen hallinnon organisaation tai näiden yhdistelmien omistuksessa tai ylläpitämänä. Palvelu tuotetaan pilvipalveluntarjoajan tiloissa. Hybridipilvi koostuu kahdesta tai useammasta erilaisesta pilvi-infrastruktuurista. Infrastruktuurit pysyvät omina yksittäisinä kokonaisuuksinaan, mutta toimivat sidottuina yhteen standardoidulla tai sovelluskohtaisella teknologialla. Ratkaisu mahdollistaa datan ja applikaatioiden siirrettävyyden esimerkiksi tilanteissa, joissa resursseja tulee tasapainottaa kahden eri pilven välillä. (Mell & Grace 2011, 2–3)

Teollisen esineiden internetin sensoridata tallennetaan yleensä pilveen fyysisen paikallisen palvelimen tai yrityksen oman konesalin sijasta. Sen eduiksi voidaan luetella tallennustilan edullisuus ja automaattinen skaalautuvuus lukemattomille laitteille. Pilvi ei datavarastona kuitenkaan aina ole paras vaihtoehto, sillä tietoturvan kannalta ajateltuna on joissain tilanteissa perustellusti parempi vaihtoehto tallentaa data paikallisesti. Paikallisesti tallennettua dataa voidaan kuitenkin analysoida yksityisessä tai julkisessa pilvessä, kunhan tietoturvasyistä siitä on siivottu ensin pois kaikki tietosuojan kannalta kriittiset elementit. Tietyissä tilanteissa pilviratkaisu ei tule kysymykseenkään, esimerkiksi kun datan käyttötarve ei siedä latenssia tai verkkoyhteydessä esiintyviä häiriöitä. Latenssikriittisissä tilanteissa kannattaa vastaavasti hyödyntää reunalaskennan tarjoamia mahdollisuuksia. (Collin & Saarelainen 2016, Luku 10)

### 3.8 Massadata

Massadata (big data) on käsite, jolla viitataan jatkuvasti kasvavaan massiiviseen tietojoukkoon. Massadataa syntyy nykypäivänä jatkuvasti monesta eri lähteestä, varsinkin sosiaalisesta mediasta, internetsivuilta, sää- ja navigointidatasta, terveydenhuollon ja erilaisten laitteiden keräämistä tiedoista. Tämä kerätty tieto voi olla strukturoitua tai ei-strukturoitua ja se voi koostua jopa kuvista, äänestä ja videosta. Tällaisen valtavan tietomäärän hallitseminen ja analysoiminen on perinteisillä tietokantatyökalujen menetelmillä käytännössä mahdotonta tai erittäin haasteellista. Massadatalle on olemassa muutamia tyypillisiä tunnusmerkkejä, jolloin puhutaan viidestä V:stä: volume (määrä), variety (valikoima), velocity (nopeus), value (arvo) ja veracity (todenmukaisuus). (Neittaanmäki & Siukonen 2019, Osa 2: Tietonurkka)

Suosittuja massadatan tallennukseen käytettyjä ratkaisuja ovat NoSQL-tietokannat ja Hadoop, joista jälkimmäinen poikkeaa luonteeltaan NoSQL-tietokannoista. Hadoop perustuu palvelinryppääseen, eli klusteriin, joka toimii hajautettuna tallennusjärjestelmänä. Kokonaisuutena se on vikasietoinen ja se on tarkoitettu isojen datamassojen tallentamiseen ja käsittelyyn. Tähän tarkoitukseen voidaan hyödyntää jopa edullisia standardikomponenteista kasattuja palvelimia, koska klusterin ainoana todellisena vaatimuksena on kattava tallennustila. Teollisen internetin käyttötarkoitukseen Hadoop-klusteri voidaan rakentaa yrityksen omaan konesaliin, mutta halvin ja helpoin tapa toteuttaa tämä on ulkoistaa ratkaisu ja ostaa se pilvipalveluna. NoSQL-tietokantoja on markkinoilla tarjolla satoja erilaisia, joilla kaikilla on omat ominaisuutensa. Myös Hadoopille on olemassa useita eri kilpailijoita. (Collin & Saarelainen 2016, Luku 11)

Tiedonlouhinta (data mining) viittaa joukkoon menetelmiä, joilla suurista tietomassoista pyritään löytämään juuri tietyn tyyppistä oleellista tietoa. Menetelmä on vahvasti yhteydessä tilastotieteeseen ja koneoppimiseen, jota hyödynnetään tahdotun lopputuloksen saavuttamiseksi. (Neittaanmäki & Siukonen 2019, Osa 2: Tietonurkka)

On hyvä muistaa, että massadata aiheuttaa myös tietoturvalle erittäin suuria odotuksia ja vaatimuksia, sillä suurten datamäärien vuotaminen vihamielisiin käsiin olisi esimerkiksi monelle pk-yritykselle vakava vastoinkäyminen.

### 3.9 Lohkoketjut

Lohkoketju (blockchain) on eräänlainen hajautettu tietokanta. Se pitää sisällään muuttumattomassa järjestyksessä olevia datalohkoja, jotka ovat linkitettyjä ja kryptografisesti suojattuja. Lohkoketjujen tieto on hajautetusti tallennettuna useaan eri kohteeseen samanaikaisesti eri solmukohtina toimivissa tietokoneissa. Tämä menetelmä varmistaa tiedon saatavuuden, säilyvyyden ja käytettävyyden. Lohkoketjut ovat luonteeltaan luottamuksettomia tietoverkkoja, mikä tarkoittaa sitä, että tieto tallennetaan useaan eri sijaintiin ja uusi tieto validoidaan sekä varmistetaan kussakin paikassa erikseen. Lohkoketjut ovat muuntumattomia ja dataa on jälkikäteen mahdotonta muuttaa tai poistaa lisäämisen jälkeen. (Neittaanmäki & Siukonen 2019, Osa 2: Tietonurkka)

Lohkoketjuista on hyötyä, kun sovelluksissa ja tilanteissa vaaditaan tapahtumien varmentamista. Hyvä käyttökohde tällaiselle ratkaisulle on verkkoon kytketyistä mittalaitteista ja antureista koostuva IoT-järjestelmä, jonka tuottamien tietojen luotettavuus ja alkuperä täytyy saada varmennettua. Lohkoketju on kuin lista toisiinsa linkitetyistä tapahtumista, jossa

tapahtumat voidaan varmentaa ja linkittää toisiinsa kryptografiamenetelmiä hyödyntämällä. Lohkoketjuja ylläpidetään hajautetusti hyödyntäen useita palvelimia ilman keskitettyä luotettua tahoa. Tämä mahdollistaa tiedon siirtymisen yksittäisestä toimijasta riippumatta. (Valtionneuvoston Selvitys- ja Tutkimustoiminta 2018, 1)

Johtopäätöksenä voidaan todeta, että lohkoketjuteknologiat voivat auttaa pk-yrityksiä liiketaloudellisesti ja tietoturvan hallinnan kannalta. Kyseisen teknologian tuomat hyödyt eivät välttämättä ole vielä konkretisoituneet, mutta tilanne on murrosvaiheessa ja näyttää lupaavalta pk-yritysten kannalta.

### 3.10 Tekoäly

Tekoälylle ei ole olemassa mitään täsmällistä ja yksiselitteistä määritettä. Se on käytännössä kokonaisuus, joka koostuu useammasta eri teknologiasta, joten sen määritelmää ei voida rajata liian tiukasti. Tekoälyllä on kuitenkin tiettyjä ominaisuuksia, kuten oppivuus, suorituskyvyn laaja-alaisuus ja autonomisuus. Tekoälyllä voidaan yleisessä mielessä käytännössä tarkoittaa koneita, laitteita, ohjelmistoja ja järjestelmiä, jotka voivat oppia ja pyrkivät tekemään päätöksiä samalla tavalla kuin ihmiset. Tekoälyteknologiat jakautuvat erityyppisiin ratkaisuihin, kuten esimerkiksi koneoppiminen, syvät neuroverkot ja konenäkö. Nykyisin käytössä olevat tekoälyt suoriutuvat ihmistä paremmin hyvin kapea-alaisista tehtävistä, mutta yleisistä laajemmista tehtävistä toistaiseksi ihminen suoriutuu vielä sitä huomattavasti paremmin. (Työ- ja elinkeinoministeriö 2020, 62–63)

Tekoälyyn on kohdistunut paljon odotuksia ja sen uskotaan tulevaisuudessa mullistavan liikennettä, teollisuutta, terveydenhuoltoa ja työelämää. Tekoälykehityksen taustalla on nopeasti kasvanut laskentakapasiteetti sekä helposti ja edullisesti saatavilla oleva data, jota voidaan soveltaa oppimateriaalina tekoälylle. Datan määrä on kasvanut huomattavasti ja siihen on vaikuttanut edullisempien sensorien saatavuus ja yleistyminen sekä tallennuskapasiteetin kasvu. (Työ- ja elinkeinoministeriö 2017, 15)

Tekoälyä voidaan soveltaa muun muassa massadataa louhittaessa. Tässä tehtävässä sovelletaan yleensä koneoppimista, mutta myös muita ohjatun oppimisen tekoälymenetelmiä voidaan soveltaa. Nämä menetelmät voivat hyödyntää esimerkiksi neuroverkkoja ja syväoppimista. (Collin & Saarelainen 2016, Luku 14)

Koneoppimisella (machine learning) tarkoitetaan tiettyä tekoälyn osa-aluetta. Sen avulla kone itse oppii toistuvien tapahtumien perusteella tulkitsemaan ja havainnoimaan asioita. Toiminnallisesti tämä perustuu monimutkaisiin algoritmeihin. Myös itse koneoppiminen

voidaan jakaa kahteen eri kategoriaan: ohjattuun ja ohjaamattomaan oppimiseen. Neuroverkko (artificial neural network) on yhdistävään laskentaan perustuva kokonaisuus, joka on suuntautunut informaation käsittelyyn matematiikan ja laskennan mallien avulla. Neuroverkkoja hyödynnetään muun muassa kuvantunnistuksessa, konenäössä, puheentunnistuksessa, kielen kääntämisessä, peleissä ja lääketieteellisten diagnoosien yhteydessä. Syväoppiminen (deep learning) pyrkii jäljittelemään ihmisen aivojen toimintaa. Se perustuu monikerroksiseen datan käsittelyyn, jossa jokaisella kerroksella on oma tehtävänsä. Neuroverkkojen koulutus vaatii suuria määriä opetusdataa, koska kyseiset verkot voivat sisältää miljoonia säädettävissä olevia parametreja. (Neittaanmäki & Siukonen 2019, Osa 2: Tietonurkka)

On huomioitava, että tekoälyä käytetään IoT-järjestelmissä ja pilvipalveluissa, mikä tarkoittaa, että se on tärkeä osa kokonaisuutta. Tietoturvan kannalta on hyvä muistaa, että tekoälylle käsiteltäväksi annettu data ja oppimateriaalina käytetty data on oltava tähän käyttöön soveliasta. Käytännössä tämä tarkoittaa, että mikään paikallinen laki tai säädös ei saa estää tämän tarpeen toteutusta. Joissain tapauksissa datasta voidaan mahdollisesti siivota pois kaikki tarpeeton tieto, joka tekee sen käsittelystä varsinkin ulkoistetuissa palveluissa paljon turvallisempaa.

# 4 Tunnistettavat tietoturvariskit ja niiden hallinta

Tässä luvussa käydään läpi, mitä opinnäytetyötä varten kerätyn dokumenttiaineiston pohjalta on selvinnyt. Tämä vaihe nojautuu myös aikaisemmin esitettyyn tietoperustaan ja siinä ilmenneisiin asioihin. Luvussa esitetään myös havaintoja ja johtopäätöksiä lähteiden sekä oman kokeman pohjalta liittyen kyseessä kulloinkin olevaan aihepiiriin.

## 4.1 Esineiden internet ja tietoturva

Vuonna 2020 Traficom ja Kyberturvallisuuskeskus suorittivat verkkoskannausta Suomessa. Suojaamattomien järjestelmien määrä oli vähentynyt aikaisempaan mittaukseen verrattuna, mutta yksittäisten suojaamattomien laitteiden määrä oli kasvanut edellisvuodesta. Mukana havaittiin olevan myös IoT-laitteita sekä suojaamattomia etätyöpöytä- ja verkkoyhteyspalveluja. (Uusiteknologia 2021a)

Tietoturvayhtiö Trend Micron tekemän selvityksen mukaan lähes joka neljäs kansainvälinen organisaatio on joutunut useaan otteeseen verkkohyökkäyksen kohteeksi vuoden 2020 aikana. Osassa hyökkäyksistä on onnistuttu tunkeutumaan organisaatioiden verkkoihin ja järjestelmiin. Riskit ovat kasvaneet myös kotiverkkoja hyväksikäyttäen koskemaan yritys- ja IoT-yhteyksiä. Selvityksessä luokiteltiin vaarallisimmiksi kyberuhiksi tietojenkalastelu ja käyttäjien manipulointi, clickjacking-hyökkäykset, kiristyshaittaohjelmat, tiedostamattomat hyökkäykset, botnet-verkot, sekä man-in-the-middle -hyökkäykset. Näiden lisäksi todetaan eniten huolta aiheuttavien asioiden olevan organisaatioiden kannalta asiakastietojen vuotaminen, luvaton pääsy immateriaali- ja taloustietoihin, asiakkaiden menettäminen, laitevarkaudet tai järjestelmävauriot. Vakavimmat riskitekijät IT-infrastruktuurissa on luokiteltu olevan organisaatioiden järjestelmien monimutkaisuus ja heikot käytännöt, välinpitämättömyys sisäpiiriläisten keskuudessa, pilvipalvelujen infrastruktuuri ja palvelutarjoajat, pätevän henkilökunnan puute, sekä viimeisenä pahantahtoiset sisäpiiriläiset. Trend Micro epäilee myös, että vuonna 2021 pilvijärjestelmät kohtaavat rajuja hyökkäyksiä. (Uusiteknologia 2020a)

Verkkorikolliset kohdistavat toimenpiteitä nykyään kotiverkkoihin yrittäessään löytää erilaisia hyökkäysreittejä yritys- ja IoT-verkkoihin. Trend Micron ennusteena on, että vuonna 2021 kotiverkot, etäyhteysohjelmistot ja pilvipalvelut ovat kyberhyökkäysten keskiössä. Tämä tarkoittaa sitä, että arkaluontoista tietoa säännöllisesti käsittelevien henkilöiden tulisi olla varuillaan nykyisen tilanteen takia, koska hyökkäyksiä kohdistetaan juuri heihin. Kohdistaminen onnistuu yleensä hyväksikäyttämällä ryhmätyö- ja tuottavuusohjelmistojen haavoittuvuuksia, jotka ovat jo ennalta tunnettuja. Kyseessä ei siis ole yleensä nollapäivä-

haavoittuvuuksista. Verkkorikollisuudelle tarjolla olevien access-as-a-service -murtopalveluiden määrän kasvaessa kasvaa koti-, yritys- ja IoT-verkkoihin kohdistuvien hyökkäysten määrä. Organisaatioille suositellut toimenpiteet tässä tilanteessa ovat, loppukäyttäjien kouluttaminen ymmärtämään yritystietoturvaa, parhaita etätyökäytänteitä ja käyttämään vain yrityksen määrittelemiä laitteita työtehtävissään. Ylläpitäjien tulisi myös rajoittaa käyttöoikeuksia yritysverkossa ja kotitoimistoissa sekä noudattaa Zero Trust -suojausmallia. Yritysten tulisi noudattaa parhaaksi havaittuja käytänteitä, huolehtia päivitystenhallinnasta ja tehostaa uhkavalvontaa. Tehtävissä on suositeltavaa käyttää asiantuntijoita, jotta pilvipalvelut, niiden työkuorma, sähköinen kommunikaatio sekä päätelaitteet ja verkot olisivat jatkuvasti suojattuja. (Uusiteknologia 2020a)

Tietoturvayhtiö Avast (2019) on yrityksille suunnatussa blogikirjoituksessa todennut, että esineiden internet tuo tehokkuutta, mutta myös uusia riskejä. Julkaisussa myös kiinnitetään huomiota siihen tosiasiaan, että IoT-laitteita ei yrityksissä suojata yleensä yhtä tunnollisesti ja tehokkaasti kuin muita laitteita. Eräs merkittävin ongelma tietoturvan kannalta esineiden internetissä on se, että sen ratkaisut sisältävät paljon verkkoon liitettyjä päätepisteitä, mikä tarjoaa laajan hyökkäyspinta-alan. Jokainen yrityksessä käyttöön otettu IoT-laite kasvattaa tuota pinta-alaa jatkuvasti, ja tilannetta vaikeuttaa se, että laitteet voivat olla ristiin yhdistettyjä, mikä lisää riskejä. Avast on määritellyt huomattaviksi IoT-tietoturvaongelmiksi yritysympäristössä arkaluontoisen tiedon vuotamisen, sabotaasin, bottiverkot ja bottiverkkoja hyödyntävät palvelunestohyökkäykset. Julkaisussa mainitaan myös, että IoT-haittaohjelmat kehittyvät jatkuvasti ja tämä uhka koskee myös pienyrityksiä. Pienyritysten, joissa käsitellään luottamuksellista asiakastietoa, tulisi olla varuillaan mahdollisen laitteiden hakkeroinnin varalta. Hakkeroidun laitteen kautta hyökkääjällä on mahdollisuus varastaa käsiteltyä tietoa. (Avast 2019)

Esineiden internetin päätepisteiden turvaaminen riippuu paljolti siitä, millaisia laitteistoja yrityksellä on käytössä, joten tiettyjen varotoimien suorittaminen parantaa tietoturvaa. IoT-laitteissa ei saa jättää käyttöön oletussalasanoja, vaan käytössä pitää olla vahva salasanakäytäntö. Vastaava vahva salasanakäytäntö tulee olla käytössä myös koko verkossa ja siihen liitetyissä muissa laitteissa. Tämä voi hidastaa tai jopa estää hyökkääjän toimia. Tärkeää on, että varsinkaan reititin ei joudu hyökkääjien hallintaan. Sen salasanakäytännöstä ja päivitysten ajantasaisuudesta on pidettävä huolta ja palomuuri on kytkettävä päälle. IoT-laitteiden vastuulliset valmistajat julkaisevat korjauspäivityksiä laitteiden ohjelmistoihin, kun niistä löydetään haavoittuvuuksia, mutta kaikki valmistajat eivät kuitenkaan ole näin vastuullisia. Tällöin on perusteltua harkita, miten tämä puute vaikuttaa koko yritykseen, mikäli sitä vastaan hyökätään. (Avast 2019)

Yrityksissä ei aina mielletä, että kontrollijärjestelmät ovat yhteydessä internetiin, mutta sitä ne kuitenkin nykyään ovat. Yhteys ei välttämättä ole millään tavalla suora, vaan kulkee epäsuorasti muiden järjestelmien kautta. Hakkereiden ja muiden vihamielisten tahojen on mahdollista tunkeutua varsinaisena kohteena oleviin järjestelmiin hyväksikäyttämällä muiden järjestelmien haavoittuvuuksia. Mikäli järjestelmiin päästään tunkeutumaan, saattaa siitä seurata suuria tappioita ja muita arvaamattomia seurauksia. Hyökkäyksien aikana tietoa voidaan esimerkiksi pyrkiä manipuloimaan tai tuhoamaan, mutta sitä voidaan myös yrittää hyödyntää muilla tavoin, ja fyysistä vauriotakin voidaan saada aikaan. (Collin & Saarelainen 2016, Luku 16)

Edeltävien asioiden perusteella käy selvästi ilmi, että uhkat ovat konkretisoituneet varsinkin pilvipalveluiden kautta, koska niitä käytetään hyvin laajalti IoT-järjestelmien toiminnallisuudessa. Kuten opinnäytetyön luvussa 3.7 käy ilmi, asiakkaan ja palveluntarjoajan vastuualueet tietoturvan kannalta vaihtelevat kulloinkin käytössä olevan pilvipalvelumallin mukaisesti. Tämä edeltävä on hyvin tärkeä havainnoida jo IoT-järjestelmää suunniteltaessa ja myös resurssimitoituksenkin takia. Esineiden internetin järjestelmiin ja laitteistoihin kohdistuvat uhkat ovat myös tietyssä mielessä hyvin perinteisiä jo aikaisemmin tunnistettuja uhkia, jotka koskevat enemmän tai vähemmän kaikkia nettiin liitettyjä laitteita tai tietokonelaitteistoja. Kuten aikaisemmin on kerrottu, nollapäivähyökkäyksistä ei pääasiallisesti ole nykytiedon perusteella ollut kysymys, vaan vanhojen tunnistettavien tietoturva-aukkojen hyväksikäyttö on edelleen vallalla oleva trendi. Johtopäätöksenä tästä voidaan todeta, että tätä trendiä vastaan on mahdollista kamppailla noudattamalla jo tiedossa olevia yleisiä suositeltuja tietoturvakäytänteitä. Kuten tämän opinnäytetyön luvun 2.3 pohjalta voidaan todeta, ovat pk-yritysten henkilöstö ja varallisuusresurssit hyvin paljon isompia toimijoita rajallisemmat. Eli mikäli yrityksessä ei ole tietoturvaosaamista omasta takaa, kannattaa silloin asiantuntijan apua hakea oman yrityksen ulkopuolelta. Muun muassa Avastin huomattavaksi uhaksi määrittelemä arkaluintoisen tiedon vuotaminen IoT-tietoturvaongelman vuoksi voi olla mahdollinen skenaario monen eri tekijän tuloksena. Tietoperustassa on muun muassa luvuissa 3.1 ja 3.7 käyty yleisesti läpi tähän kyseiseen uhkaan liittyviä seikkoja ja kuinka siihen liittyviä riskejä voidaan pyrkiä minimoimaan. Kyseessä on tietoperustaan perustuen datan käsittelyyn ja tallentamiseen sekä erinäisiin laitteiden ja datan käyttöoikeuksiin liittyvä tietoturvariski.

Internetiin suoraan kytkettyjä laitteita voi löytää Shodan-hakupalvelun avulla. Palvelu toimii periaatteessa samalla tavalla kuin mikä tahansa muukin hakukone, mutta erona on se, että Shodan on erikoistuneempi tällaisiin asioihin. Palvelu indeksoi löydettyjä laitteita ja niihin liittyviä julkisia tietoja. Löydetyt laitteet voivat vaihdella pienistä yksittäisistä laitteista aina ydinvoimaloihin saakka. (Shodan 2020)

Mikäli yrityksen käytössä olevaa laitteistoa näkyy Shodan-hakupalvelussa, on se erittäin selvä merkki siitä, että yritys ei ole valmis soveltamaan esineiden internetiä. Shodan mahdollistaa verkkoon liitettyjen turvattomien, huonosti konfiguroitujen ja verkkoon näkyvien laitteiden löytämisen. Tietoturvan kannalta tämä on erittäin huono asia, sillä kuka tahansa voi etsiä ja löytää näitä laitteita kyseisen palvelun kautta. Palvelun kautta löytyy reitittimiä, tulostimia, valvontakameroita ja jopa teollisuuden SCADA-laitteistoja. Tästä laitteiden joukosta löytyy myös suomalaisia kohteita, joiden IP-osoitteet ovat näkyvillä palvelun kautta. (Collin & Saarelainen 2016, Luku 15)

On erittäin tärkeää varmistaa, ettei yrityksen käyttämiä esineiden internetiin kuuluvia laitteita ole löydettävissä tarkoituksettomasti kyseisen palvelun kautta. Jos laitteita näkyy palvelussa, on melko varmaa, että rikollisetkin tietävät tästä ennemmin tai myöhemmin. Tämä myös mahdollistaa suorat tai epäsuorat hyökkäykset yrityksen käytössä olevia laitteistoja kohtaan. Juuri tästä syystä on tärkeää, että yrityksissä ymmärretään, kuinka laitteiden asetukset tulee olla määritettynä. Mikäli ymmärrystä ei ole, niin se mahdollistaa suurella todennäköisyydellä vihamielisten tahojen haitalliset toimet.

Uusia hyökkäysvektoreitakin tulee jatkuvasti lisää muun muassa IIoT-järjestelmiin. Näitä vektoreita hyväksikäyttämällä voidaan mahdollisesti pyrkiä levittämään kiristyshaittaohjelmia tai vastaavasti pyrkiä suorittamaan jopa teollista vakoilua sekä sabotaasia. Tilanne johtuu usein siitä, että yrityksissä oletetaan virheellisesti älytuotannossa käytettyjen laitteiden toimivan omassa verkossa eristyksissä muusta internetistä. Todellisuudessa nämä laitteet ovat organisaation käyttämien IT-järjestelmien kautta yhteydessä normaaliin verkkoon ja siten myös mahdollisesti hakkereiden saavutettavissa. Tutkijoiden mukaan, tietyissä tilanteissa hakkereiden on teoriassa ollut mahdollista hyödyntää älylaitteiden tuotannossa käytettyjä sovelluskehitysalustojen haavoittuvuuksia. Tämä siis mahdollisti laitteiden tuotantoprosessin saastuttamisen ja hyväksikäyttämisen. Tämä kyseinen tutkijoiden löytämä tietoturva-aukko on sittemmin korjattu, mutta vastaavia ja muita hyökkäysvektoreita on lisääkin. Esimerkiksi tietyissä tilanteissa hakkerin on mahdollista muokata käytettyjen sensorien valvontadataa, niin että sillä saadaan erilaista haittaa aikaiseksi kohteessa. Toisin sanoen väärennettyä dataa voidaan pyrkiä käyttämään yrityksen verkossa peittelemään todellista tapahtunutta. Koska näitä uusia hyökkäysvektoreita kehittelevät rikolliset eivät vain istu ja odota sopivan kohteen löytymistä, pitää laitteita pyrkiä tehokkaasti suojaamaan kohteissa, joissa hyödynnetään teollista internetiä. Järjestelmiä kohtaan suunnatut uhat lisääntyvät, koska älyä hyödyntävissä järjestelmissä kaikki osat ovat yhä riippuvaisempia toisistaan. Perinteisissä tapauksissa tietoturvaa voidaan parantaa huomattavasti päätelaitteiden säännöllisen tarkastuksen avulla, mutta teollisen internetin

kohdalla tilanne on mutkikkaampi. Valvonnan tehostaminen, käytettyjen verkkojen mahdollinen erottelu ja säännöllinen laitteistojen testaaminen auttavat kuitenkin riskien hallinnassa. (Mikrobitti 2020)

Vaikka uusia hyökkäysvektoreita kehitelläänkin jatkuvasti esineiden internetiä kohtaan, niin voidaan tästä vetää johtopäätös, että tehokkaalla valvonnalla ja muulla ennaltaehkäisevällä toiminnalla voidaan minimoida riskejä tehokkaasti. Huomiota kannattaa myös kiinnittää esineiden internetin teknologiapinon viidenteen tasoon, eli sovellustasoon, jota on käyty läpi tämän opinnäytetyön tietoperustassa luvussa 3.1. Aikaisemmin kuvattu tietoturvaongelma nimittäin tuo esille hyvin konkreettisesti sen, miksi sovelluskehityksessä oikeuksien antaminen eri tahoille kannattaa miettiä ja säännöstellä tarkkaan, ettei vastaavaa pääsisi tapahtumaan. Edeltävästä käy ilmi myös hyvin se, miten kehnosti valvotussa verkossa jopa sensorien tuottamaa dataa voidaan hyväksikäyttää. Mielestäni tämä konkretisoi puolestaan erittäin hyvin, miksi turvallisen verkon suunnitteluun, toteutukseen ja ylläpitoon pitää panostaa kaikissa yrityksissä. Tietoturvan kannalta oikeuksien hallinta tulee ottaa vakavasti kaikissa ympäristöissä.

Kaiken edeltävän jälkeen on todettava, että tietoturvan suhteen ei voi olla vain reaktiivinen, vaan nykyään on pyrittävä proaktiiviseen rooliin tietoturvan ylläpidossa.

### 4.2 Tietoturvallisuus pk-yrityksissä

Verkkorikollisuus on kasvussa jatkuvasti ja samalla sen kohteeksi joutumisen riski on suurentunut huomattavasti. Rikolliset pyrkivät käyttämään hyödyksi tiedossa olevia haavoittuvuuksia, jonka takia tähän on organisaatioiden taholta pyrittävä vastaamaan päivittämällä tietojärjestelmiä ja sovelluksia yhä nopeammassa tahdissa. Huijauksista kärsivät myös useat eri tahot ja organisaatiot, riippumatta siitä onko kohde pk-yritys vai jokin isompi toimija. Tietoturvan hoitaminen tuo täsmällisyyttä kaikkeen tekemiseen yrityksissä. Se myös mahdollistaa parempien ja turvallisempien palveluiden tarjoamisen asiakkaille. Pelkästään perusasioista huolehtimalla voidaan tietoturvariskejä minimoida tehokkaasti. (Databros 2020)

Yleisimpiä pk-yritysten tietoturvaongelmia ovat yrityksen johtoportaan osalta puutteellinen ymmärrys tietoturvariskeistä, suoritetun valvonnan ja hallinnan puutteellinen toteutus, haavoittuvuuksia ei korjata systemaattisesti, seuranta on puutteellista, tiedonhallinta kärsii liian ulkoistamisen vuoksi, sekä epäselvät vastuualueet siitä, kuka vastaa, mistä ja miten. Käyttäjien osalta tunnistettavia tietoturvariskejä ovat erinäiset sähköpostikäytänteisiin liittyvät riskitekijät, kuten esimerkiksi haitalliset linkit ja salaamattomat viestit. Tämän lisäksi

käyttäjien osaamattomuus tai huolimattomuus sekä rajaamattomat oikeudet katsotaan tietoturvaongelmiksi pk-yrityksissä. Käyttäjien tulisi myös noudattaa vahvoja salasanakäytänteitä ja oletussalasanoista täytyy hankkiutua eroon. Laitteiden kohdalla tietoturvaongelmina ovat avoimet wifi-yhteydet, mobiililaitteiden suojaamattomuus, mahdolliset mobiililaitteiden katoamiset ja varkaudet, tietoturvattomat IoT-laitteet, heikko suojautuminen nettiuhkia vastaan, laitteiden käyttöönottoon ja ylläpitoon liittyvät puutteet, käytöstä poistettavien laitteiden sisältämät tiedot sekä parhaiden varmuuskopiokäytänteiden laiminlyöminen. Parempaan tietoturvaan voidaan päästä pk-yrityksissä laatimalla käytännöt ja roolit sekä kouluttamalla valitut henkilöt hoitamaan näitä rooleja. Kun selkeät toimintasuunnitelmat ja ohjeistukset eri tilanteisiin on luotu, vähentää se riskejä huomattavasti. Dokumentaatiolla on keskeinen rooli tässä kaikessa ja se pitäisi pyrkiä pitämään ajan tasalla, jolloin asiakkaille ja viranomaisille voidaan esittää toteen toimenpiteiden kattavuus. Tämän edeltävän lisäksi tiedon hallinta tulisi yksinkertaistaa, eli tiedon koko elinkaari on selvitetty ja sen tallentamiseen sovelletaan keskitettyä ratkaisua. Vain tarpeellinen tieto tallennetaan ja tiedon käsittelylle sekä jakamiselle otetaan käyttöön selkeät säännöt. Arkaluontoiset tarpeettomat tiedot tulisi tuhota aina asianmukaisia turvallisia menetelmiä soveltaen. (Databros 2020)

Erilaisten ratkaisujen hallitseminen keskitetysti helpottaa jatkuvan seurannan toteuttamista, laitteiden ja palveluiden käyttöönottoa sekä päivityskäytänteiden noudattamista. Keskitetty hallinta on tärkeää erityisesti IoT-laitteiden kanssa, sillä niiden asianmukainen suojaaminen on tärkeää. Missään nimessä IoT- ja verkkolaitteissa ei saisi olla käytössä oletussalasanoja. Verkon turvallisuudesta huolehtiminen kuuluu myös osaksi hyvää keskitettyä hallintaa. Ongelmatilanteisiin on varauduttava jo ennen niiden kohtaamista, eli erilaisten toimintasuunnitelmien luominen ja noudattaminen auttavat tämän päämäärän saavuttamisessa. Hyviä varmuuskopiointikäytänteitä tulisi noudattaa automatisoimalla niihin liittyvät prosessit mahdollisimman pitkälle. Hyviin käytäntöihin kuuluu myös varmuuskopioiden toimivuuden testaaminen tietyin väliajoin, mikä varmistaa nopeamman palauttamisen tarvittaessa. Varmuuskopioita voidaan tallentaa organisaation omille palvelimille tai pilvipalvelimille. Mikäli tärkeää tietoa halutaan säilöä erillisillä mukaan otettaville tallennusvälineille, pitäisi ne aina suojata vahvalla salasanalla. (Databros 2020)

Ei ole riittävää, että tietoturvallisuuteen liittyvät asiat on vain kerran toteutettu, vaan tilannetta täytyy seurata ja kartoittaa jatkuvasti. Tämä johtuu siitä, että tietoympäristö on jatkuvassa muutoksessa ja tähän muutokseen on yrityksessä pystyttävä aina vastaamaan. Kyseiseen tehtävään on valtuutettava joku asiantuntijataho, joka voi olla yrityksessä toimiva oma tietoturvavastaava tai joku ulkopuolinen asiantuntija. Tarvittavaan seurantaan ja kar-

toitustyöhön on olemassa erilaisia automatisoituja työkaluja, jotka auttavat pysymään selvillä tietoturvatilanteesta yritysympäristössä. Organisaatioon kuuluvien henkilöiden tulisi aina ilmoittaa omista tietoturvaan liittyvistä havainnoistaan muille, jotta mahdollisia ongelmia voidaan ennaltaehkäistä tehokkaasti ja ajoissa. Kaikista muutoksista tietoympäristössä ja tietoturvatilanteessa tulisi aina raportoida niin, että muutos saadaan organisaatiossa yleiseen tietoisuuteen. (Databros 2020)

Liikenne- ja viestintävirasto Traficom (2020) on julkaissut pienyritysten kyberturvallisuusoppaan. Opas on pääasiallisesti suunniteltu alle 50 työntekijän yrityksille ja se pitää sisällään paljon käsitteitä ja määritelmiä. Itse suositellut toimenpiteet ovat samassa linjassa aikaisemmin kuvailtujen toimenpiteiden kanssa. Huomioitavaa kuitenkin on, että opas ei ota suoraan kantaa esineiden internetiä koskeviin asioihin, vaan on yleinen kyberturvallisuusopas pienyrityksille, joka auttaa ymmärtämään tarvittavat perusasiat. Aikaisemmin kuvailtujen toimenpiteiden lisäksi, yleisenä turvallisuustoimena opas suosittelee monivaiheisen tunnistautumisen käyttämistä yrityksen sisäisissä ja ulkoisissa palveluissa, koska se parantaa huomattavasti turvallisuutta.

Liikenne- ja viestintävirasto Traficom (2019) on myös julkaissut erittäin yleispätevän ohjeistuksen ”Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille”. Kyseisessä oppaassa on koottu yhteen erilaisia pilvipalveluiden tietoturvaan liittyviä tärkeitä asioita ja konsepteja. Siinä keskitytään tarkastelemaan tietoturvaan liittyviä asioita käytettävyyden, luottamuksellisuuden ja eheyden näkökulmasta. Ohjeistuksen tarkoitus on auttaa tilanteessa, jossa esimerkiksi pienyrityksen taholla pohditaan erilaisten pilvipalveluiden käyttöönottoa. Teoksessa suositellaan myös tutustumista edistyneempään ohjeistukseen tarvittaessa nimeltä PiTuKri, joka on myös Traficomin julkaisema ohjeistus. PiTuKri on suunnattu lähinnä viranomaisohjeistukseksi, mutta Traficom suosittelee myös muiden tahojen, kuten pienyritysten tutustuvan sen sisältämiin pilvipalveluiden turvallisuuteen ja turvallisuuden arviointiin liittyviin asioihin, sekä tutkimaan näihin liittyviä hyviä käytäntöjä.

Kyseinen ohjeistus on varsin kattava ja siitä on hyvä lähteä liikkeelle pienyrityksen kohdalla, kun tarvitaan kattavaa perustietoa pilvipalveluiden valintaa koskien. Ohjeistus on yleistasostaan huolimatta tarpeeksi pätevä toimiakseen myös erittäin hyvänä lähtökohtana tilanteissa, joissa tarkoituksena on ottaa käyttöön pilvipalvelut esineiden internetin käyttöä varten. Tietoturvan kannalta ohjeistuksessa on erinomaisesti tuotu esille riskienhallintaa koskevat asiat.

Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille -oppaassa todetaan, että pilvipalveluien tietoturvallisuuden varmistumiseen liittyy haasteita. Tämä johtuu siitä, että muun muassa pienyrityksillä ei ole mahdollisuuksia lähteä toteuttamaan tietoturvallisuuskäytäntöjen syvällistä arviointia palveluntarjoajan suhteen. Näissä tilanteissa yleensä täytyy nojautua palveluntarjoajan suorittamiin itsearviointeihin, sertifiointeihin ja sopimusteknillisiin sitoumuksiin. Tästä syystä Kyberturvallisuuskeskus on tuottamassa selvitystyötä, jossa pyritään selvittämään, kuinka tulevaisuudessa voitaisiin paremmin tukea pienten toimijoiden tilannetta edeltävän kannalta. (Liikenne- ja viestintävirasto Traficom 2019)

Edeltävä toimii hyvänä esimerkkinä siitä, että yrityksissä tulisi suhtautua hyvin kriittisesti palveluntarjoajien lupauksiin, ellei niitä voida näyttää toteen selvällä ja yksiselitteisellä tavalla. Tämä on tärkeä asia mieltää osaksi suurempaa riskienhallintakokonaisuutta yrityksissä.

Esineiden internetiä koskevaa yleispätevää ohjeistusta ei valitettavasti ole saatavilla esimerkiksi Traficomilta, koska kyseessä on luvussa 2.4 havainnoidulla tavalla vielä varsin kehitysvaiheessa oleva teknologia. Kaikkia siihen liittyviä asioita ei siis ole vielä tunnistettu tai standardisoitu tarpeeksi pitkälle. Standardeista on mainittu aikaisemmin esitetyssä tietoperustassa useammassa kohdassa, eri yhteyksissä, mutta tilannetta on kuvattu esineiden internetin kohdalla yleisesti luvussa 3.4. On kuitenkin pidettävä mielessä, että asiat muuttuvat kaiken aikaa ja ohjeistuksia päivitetään jatkuvasti. Uutisten ja tuoreiden ohjeistusten seuraaminen varsinkin Traficomin ja Kyberturvallisuuskeskuksen taholta on suositeltavaa Suomessa toimiville pk-yrityksille ja muillekin kiinnostuneille tahoille. Traficom tarjoaa kätevästi ajankohtaista tietoa sivustoillaan, liittyen juuri ajankohtaisiin tietoturvauutisiin ja ohjelmistohaavoittuvuuksiin (Liikenne- ja viestintävirasto Traficom 2021). Se on siis hyvä paikka lähteä hakemaan tuoretta laadukasta tietoa, joka liittyy tietoturvaan.

Suomessa varsinkin operaattorit tarjoavat yritysasiakkaille erilaisia ulkoistettuja tietoturvapalveluita ja ratkaisuja. Näiden tarjottujen palveluiden kautta yritysten on mahdollista saavuttaa erilaisia asiantuntijatason ratkaisuja, jotka helpottavat yritysten päivittäistä toimintaa tietoturvan kannalta katsottuna. Kyseiset ratkaisut ovat tarkoitettuja turvaamaan yrityksen tietoliikennettä ja säästämään yrityksen omia sisäisiä resursseja tässä tehtävässä. Osa palveluista mahdollistaa myös automatisoituja prosesseja, joilla pyritään tunnistamaan ja estämään verkon kautta tapahtuvia hyökkäyksiä. Tarjolla on myös erilaisia palvelunestohyökkäyksiä vastaan tarjottuja palveluita, pilvipohjaisia tietoturvaratkaisuja, hallinnoituja palomuuriratkaisuja, turvallisia etäyhteyksiä ja pääsynhallintaratkaisuja. (DNA 2021a; DNA 2021b; DNA 2021c; DNA 2021d; Elisa Oyj 2021a; Telia Company 2021a)

Tästä kaikesta edeltävästä on mahdollista päätellä, että erilaisista ohjeistuksista voi saada selvää hyötyä pk-yrityksessä päätöksenteon tueksi. Samalla voidaan päätellä, että kun tietoturvan perusasiat ovat yritysympäristössä kunnossa, niin se minimoi tietoturvaan liittyviä riskejä jo erittäin tehokkaasti. Koska pienemmissä organisaatioissa, kuten pk-yrityksissä resurssit eivät ole rajattomia, on mahdollista asiantuntijapalveluita hankkia oman organisaation ulkopuolelta. Tämä on mainio vaihtoehto varsinkin silloin, jos organisaation sisällä ei ole tarpeeksi osaavaa väkeä toteuttamaan kaikkea tarvittavaa tietoturvan kannalta katsottuna.

### 4.3 Esimerkki IoT-järjestelmien haavoittuvuudesta

Omana havaintona ja kokemuksena IoT-laitteistojen heikosta tietoturvatasosta on, että omassa asuintalossani otettiin käyttöön viimevuoden lopussa järjestelmä, joka näyttää erilaisia tarpeellisia tietoja talosta ja sen ulkopuolelta. Normaalissa tilanteessa talon digitaalinen infotaulu näyttää sään, bussiaikataulut, tiedotteet, asukkaiden nimet ja talosta saatavia anturitietoja, mutta mennessäni taannoin ohi tästä infotaulusta, huomasin sen olevan hakkeroitu (Kuva 8). Kyseisen järjestelmän tietoturvataso ei siis oletettavasti ollut tarvittavan korkealla tasolla. En saanut selvitettyä, mikä yritys vastaa kyseisen infotaulun toiminnasta, mutta paikallinen huoltoyhtiö ainakin otti vastaan ilmoitukset asiasta. En siis suoraan uskalla sanoa minkä kokoinen yritys lopulta järjestelmästä vastaa, mutta omana päätelmänä on, että oli yritys sitten minkä tahansa kokoinen, niin vastaavaa voi tapahtua muillekin. Tämä mielestäni myös näyttää erittäin hyvin sen mitä IoT-laitteiden kanssa voi tapahtua, mikäli haavoittuvuuksia ei tiedosteta tai hoideta kuntoon. Kyse voi olla myös tahattomasta virheestä, joka johti tapahtuman mahdollistamiseen, mutta mielestäni tämän laatuinen virhe olisi ollut mahdollista välttää hyvän tietoturvasuunnittelun avulla. Tämä kaikki on kuitenkin pelkkää spekulaatiota laajemman tiedon puutteessa.

Kuva 8. Hakkeroitu IoT-järjestelmään kuuluva infotaulu.

Itselleni tämä tapaus herätti hieman epävarmuutta suomalaisten yritysten osaamisesta tietoturvan ja IoT-järjestelmien suhteen. Ilmeisesti kehittämisen varaa tässä asiassa on, mutta toivottavasti asiasta vastaavassa yrityksessä otetaan opiksi tästä, ennen kuin jotain laajempaa tietoturvaan negatiivisesti liittyvää pääsee tapahtumaan.

### 4.4 IoT- järjestelmän käyttöönotto

Ennen IoT-järjestelmän käyttöönottoa tietoturvan kannalta katsottuna, tulisi toteuttaa laaja yksityiskohtainen kartoitus, joka koskee kaikkia jo käytössä olevia laitteita ja järjestelmiä. Kartoituksen perusteella saadaan muodostettua verkkotopologiamalli, joka on osa yrityksen sisäistä dokumentointia. Samalla on suositeltavaa toteuttaa myös tietoturvalle oma auditointi, johon kuuluu myös yrityksen nykyisen verkon auditointi. Mikäli yrityksessä on käytössä hajanainen joukko eri yhteyksiä, joita käytetään monien eri laitteiden kanssa, tulee ne jatkossa keskittää helpommin hallittavaksi kokonaisuudeksi. Muussa tapauksessa järjestelmät jäävät todella riskialttiiksi. Palomuurit ja usean kerroksen suojaus, sekä päivitysten hallinta tulee olla kunnossa ja tämän lisäksi yrityksessä tulisi noudattaa järkevää tietoturvapolitiikkaa. Tunnistautuminen on tärkeässä roolissa, jotta käyttäjät ja heille myönnetyt oikeudet pysyvät hallinnassa. Tilanne saattaa olla haastavampi, mikäli verkossa on käytössä paljon laitteita, mutta se on kuitenkin hallittavissa, käyttäen automatisaatiota apuna ja soveltamalla tähän prosessiin esimerkiksi SSH-avaimia ja asianmukaisia hallin-

tatyökaluja. Verkkoyhteyksiä on mahdollista rajata toteuttamalla ne yksi- tai kaksisuuntaisesti. Kohteissa, joissa ei tarvita kaksisuuntaista tietoliikennettä, tulisi suosia yksisuuntaista ratkaisua, mikäli halutaan saavuttaa parempi tietoturva ja minimoida riskejä. Kaksisuuntaista tietoliikennettä tarvitaan ehdottomasti kohteissa, joissa tarvitaan etähallintaa. Näissäkin tilanteissa on mahdollista toteuttaa yhteys niin, että kaksisuuntaisuus aktivoidaan vain tarvittaessa. Tietoliikenteen tietoturvan kannalta ainoastaan tarvittavien porttien tulisi olla auki ja yhteyspyynnöt tulisi sallia vain ennalta määritellyistä kohteista. Tämä tarkoittaa, että valtuuttamattomien laitteiden välisiä yhteyksiä ei sallita. Moderneja turvallisia standardeja ja protokollia tulee suosia, koska ne lisäävät tietoturvallisuutta olennaisesti. Eräät protokollat, kuten esimerkiksi OPC-UA on suunniteltu turvalliseksi käyttää ja se hyödyntää toiminnassaan sertifikaatteja ja laitelistaa, joiden kautta tiedetään mikä kommunikaatio eri laitteiden välillä on sallittua ja mikä ei. Tietyissä tilanteissa on myös mahdollista eristää järjestelmiä kokonaan pois verkosta, mutta kyseinen vaihtoehto on ääritilanneratkaisu, jota tulisi käyttää vain harkitusti. Näistä kaikista tietoturvaan, verkkoon ja järjestelmiin liittyvistä toteutetuista ratkaisuista on pidettävä yllä yrityksen sisäistä dokumentaatiota. (Collin & Saarelainen 2016, Luku 16)

Operaattorit ovat alkaneet tarjota Suomessa kattavia paketteja erikokoisiin IoT-ratkaisuihin tai räätälöivät näitä myös yritysasiakkaille aina tarpeen mukaan. Eräät palveluntarjoajat mahdollistavat jopa kokeilupakettien muodossa teknologian testaamisen ennen varsinaista käyttöönottoa. Ratkaisuissa voidaan hyödyntää mahdollisuuksien mukaan julkisia pilvialustoja, kuten esimerkiksi Azuren IoT-alustaa tai vastaavaa vaihtoehtoa. Näiltä palveluntarjoajilta on yleensä saatavana erilaista opastusta, oppaita ja joskus suoraa konsultaatiota IoT:n käyttöönottoon ja tietoturvaan liittyen. (DNA 2021e; Elisa Oyj 2021b; Telia Company 2021b; Telia Company 2021c)

Riippuen siis yrityksessä vallitsevasta osaamistasosta ja resursseihin liittyvistä tekijöistä, tässäkin tapauksessa voidaan tavoitella hyötyä mahdollisen ulkoistamisen tai asiantuntijatahon avustuksen kautta. Tähän liittyvillä päätöksillä on suora vaikutus tietoturvaan ja siihen, mitkä osa-alueet kuuluvat millekin sopijaosapuolelle. On myös hyvä säilyttää tietty kriittisyys palveluntarjoajien kuten operaattoreiden lupauksiin, koska täytyy muistaa, että he saavat tulonsa myymällä omaa tuotettaan eli tuotettua palvelua. Pk-yrityksissä kannattaa kartoittaa ja dokumentoida kaikki tarpeet ja kehityskohteet ennen ulkoisten palveluiden käyttöönoton harkitsemista, koska se selkeyttää tilannetta huomattavasti.

### 4.5 Tulevaisuuden näkymät

VTT:n joulukuussa 2020 teettämän kyselyn perusteella voidaan todeta, että suomalaiset valmistavan teollisuuden pk-yritykset ovat haluttomia investoimaan uuteen teknologiaan.

Kyselyyn osallistui 200 alan yritystä, ja vain yksi kolmasosa vastanneista pk-yrityksistä ilmoitti hakevansa kasvua ja uutta liiketoimintaa uuteen teknologiaan investoimalla. Kyseistä tulosta voidaan luonnehtia huolestuttavaksi. Investointihaluttomuus johtuu osittain ammattitaitoisen työvoiman huonosta saatavuudesta, mikä tulee johtamaan tuottavuuden laskuun ja yritysten kilpailukyvyn heikkenemiseen. Muutos tähän tilanteeseen edellyttää digitalisaation viemistä pidemmälle yrityksissä sekä investointeja automaatioon ja robotisaatioon. Tämä tavoite tarkoittaa, että yhteistyötä pitäisi lisätä pk-yritysten ja tutkimusorganisaatioiden välillä. VTT on tästä syystä mukana hankkeissa, joiden uskotaan parantava digitalisaatioratkaisujen ja uusien teknologioiden käyttöönottoa. (Uusiteknologia 2021b)

Kesäkuussa 2020 käynnistetty CHARM-projekti (Challenging environments tolerant Smart systems for IoT and AI) on saanut rahoitusta Euroopan Unionilta ja hankkeeseen kuuluu kymmeniä toimijoita EU-alueelta. Mukana on kaikkiaan 11 pk-yritystä, 14 suuryritystä ja 12 tutkimus- ja teknologiaorganisaatiota. Suomessa projektikoordinaattorina toimii Valmet. Tämän eurooppalaisen partneriverkoston tehtävänä on kehittää asiakkaille kyseisen projektin myötä uusia langattomia energiansiirtosovelluksia sekä etäyhteys- ja kyberturvallisuusratkaisuja. Näiden lisäksi on myös tulossa uusia antureita alan eri yritysten sovelluksiin. Hankkeessa on edustettuina koko IoT-ratkaisujen arvoketju: komponentti-, laite- ja järjestelmäsimuloinnit, elektroniikan materiaalit, sensorit ja komponentit, laite- ja järjestelmäintegrointi, luotettavuusanalyysit sekä pilvi- ja kyberturvallisuuden palvelut. (Uusiteknologia 2020b)

Edeltävästä on mahdollista päätellä, että Suomessa eri organisaatiot ovat ottaneet tavoitteeksi vastata nykyisiin ja tuleviin haasteisiin viemällä IoT-teknologiaa eteenpäin. Erinäisten yhteistyöhankkeiden tulokset tulevat konkretisoitumaan vasta tulevaisuudessa, mutta nämä ovat tärkeitä askelia alati digitalisoituvassa yhteiskunnassa.

# 5 Yhteenveto

Tietoturvasta ja siihen liittyvistä osa-alueista puhutaan kautta koko tämän opinnäytetyön. Kyseinen yhteenveto on tarkoitettu toimimaan tiivistettynä ja pelkistettynä kuvana tästä todella laajasta kokonaisuudesta. Tässä luvussa pyritään tuomaan esille keskeisimpiä asioita tutkimuskysymysten kannalta, jotka on esitetty aikaisemmin tämän työn johdannon osana. Yleisesti tietoturvaan liittyviä asioita ja toimintoja on esitetty opinnäytetyön luvussa 2.1, jonka jälkeen luvussa 2.2 on kuvattu kokonaisuutena esineiden internetiä. Luvun 3 alaluvuissa on taas esitetty yksityiskohtaisemmin esineiden internetiin, sen tietoturvaan ja oheisteknologioihin liittyviä asioita.

Ensimmäinen tutkimuskysymys on: mitä tunnistettavia tietoturvariskejä ja ehkäisykeinoja pk-yritysten tulisi huomioida esineiden internetin suhteen? Tähän voidaan tietoperustaan ja empiriaan perustuen todeta yhteenvetona, että erilaisia tietoturvariskejä ja niiden ehkäisykeinoja on paljon erilaisia. Kuitenkin yleisiin tunnistettaviin pk-yrityksiä koskeviin tietoturvariskeihin lukeutuvat lukujen 4.1 ja 4.2 mukaan muun muassa, että: suojaamattomia ja heikosti suojattuja esineiden internetiin kuuluvia laitteita näkyy Shodan-hakupalvelun kautta, suorat hyökkäykset IoT-laitteita kohtaan, muiden järjestelmien kautta toteutettavat epäsuorat hyökkäykset IoT-laitteita kohtaan, heikot noudatettavat tietoturvakäytännöt, työntekijöiden välinpitämättömyys, pilvipalvelujen tietoturvallisuuteen liittyvät ongelmat, pätevän henkilökunnan puuttuminen, pahantahtoiset sisäpiiriläiset, kohdistetut hyökkäykset henkilökuntaa kohtaan (tietojen kalastelu), käytetyissä ohjelmistoissa esiintyvät haavoittuvuudet, IoT-laitteistojen määrän tarjoama laaja hyökkäyspinta-ala, bottiverkot, palvelunestohyökkäykset, IoT-haittaohjelmat, laitteiden hakkerointi ja tietovarkaudet, sabotaasi ja fyysisten tuhojen aiheuttaminen, IoT-järjestelmän sensoridatan muokkaus ja hyväksikäyttö peittelemään hyökkäyksiä ja muuta toimintaa sekä IoT-järjestelmissä kohtuu harvinaiset nollapäivähyökkäykset.

Edellä mainittuja tietoturvariskejä voidaan ehkäistä tehokkaasti noudattamalla yleisesti hyviä tietoturvakäytänteitä ja -suosituksia pk-yrityksissä. Tämä aihe on käsitelty laajemmassa mittakaavassa aikaisemmissa luvuissa 4.1 ja 4.2. Hyviin tietoturvakäytänteisiin kuuluu: loppukäyttäjien koulutus ymmärtämään yritystietoturvaa riittävällä tasolla, etätyökäytänteistä sopiminen ja niiden noudattaminen, vain hyväksyttyjen laitteiden käyttäminen työasioihin, käyttäjien oikeuksien rajoittaminen yritys- ja kotiverkossa vain tarvittuihin ja perusteltuihin oikeuksiin, monivaiheisen tunnistamisen käyttäminen palveluissa, uhkavalvonnan tehostaminen, hyvien salasana- ja päivityksenhallintakäytänteiden noudattaminen,

laitteistojen säännöllinen tarkastaminen ja testaaminen, ennakoiva tietoturvatoiminta, jatkuva tilanteen seuranta ja kartoitus sekä aiheeseen liittyvän yrityksen sisäisen dokumentaation ylläpitäminen.

Riippuen pk-yrityksen toimialasta, käytettävistä järjestelmistä ja käsiteltävästä datasta, voi yrityksessä olla järkevää ottaa käyttöön Zero Trust -suojausmalli, jolloin kaikki käyttäjien toimenpiteet verkossa pitää aina hyväksyä erikseen. Tämä saattaa kuitenkin olla ylilyönti tietyillä toimialoilla ja käyttötarkoituksissa, mutta toisaalta se saattaa myös olla tietyissä käyttötarkoituksissa hyvinkin kriittinen ja tärkeä asia toteuttaa. Kuten luvun 3 alaluvuissa on kerrottu, tulee IoT-järjestelmän teknologiapinon kaikkien tasojen tietoturva suunnitella aina sopivaksi haluttuun käyttötarkoitukseen. Teoriataustan luvuissa myös mainitaan, että ei ole olemassa mitään yhtä ja samaa ratkaisua, joka soveltuu kaikkiin käyttötarkoituksiin. Pk-yrityksissä on myös hyvä muistaa, että verkon ja järjestelmien auditointi on myös tietoturvan kannalta tärkeää. Kuten luvusta 2.3 käy ilmi, ovat pk-yritysten resurssit varsin rajalliset, joten ulkoistaminen tulee tiettyjen palveluiden osalta kysymykseen tilanteissa, joissa palvelun tuottaminen sisäisesti ei ole resurssien takia mahdollista. Itse IoT-laitteistot tulisi hankkia luotetuilta ja vastuullisilta valmistajilta, jotta voidaan varmistua siitä, että laitteistojen tietoturvataso on tarpeeksi hyvä ja ohjelmistojen korjauspäivitykset olisivat saatavilla myös pitkällä aikavälillä.

Toinen tutkimuskysymys on: minkälaista tietoturvasuunnittelua pk-yrityksissä tulisi noudattaa esineiden internetin kanssa? Tähän voidaan yhteenvetona todeta, että pk-yrityksissä tulee kartoittaa aluksi nykyisin jo olemassa olevat ratkaisut ja järjestelmät, sekä luoda tästä sisäinen kattava dokumentointi. Ennen IoT-järjestelmän käyttöönottoa on myös suositeltavaa suorittaa yrityksen tietoturvaa ja yrityksen verkkoa koskevat auditoinnit, kuten luvussa 4.4 on kerrottu. Luvun 3 alaluvuista, sekä luvuista 4.1, 4.2 ja 4.4 käy ilmi, että tietoturvasuunnittelussa tulee ottaa huomioon muun muassa seuraavia asioita: sisäisen dokumentoinnin luominen ja ylläpitoprosessien suunnittelu, erilaisista käytännöistä ja henkilökunnan rooleista sopiminen, millaista kolutusta tehtäviin tarvitaan, toimintasuunnitelmat ja ohjeistukset eri tilanteisiin, tallennettavan tiedon elinkaaren selvittäminen (mitä, miksi ja minne dataa tallennetaan), tiedon tallentamisen käytännöt, tarpeellisen tiedon luokittelu, tarpeettoman tiedon tuhoaminen asianmukaisesti, hallinnoinnin suunnittelu (mielellään keskitetty ratkaisu), päivityskäytänteiden suunnittelu, salasanakäytänteiden suunnittelu, varmuuskopiokäytänteiden suunnittelu, varmuuskopioiden testaus- ja automatisointikäytänteet, tilanneseurannan ja -kartoituksen käytänteet, tietoturvapoikkeamien raportointikäytännöistä sopiminen.

Mikäli yrityksessä päätetään rakentaa kokonaan oma IoT-järjestelmäratkaisu, tulee tietoturva tällöin suunnitella jokaisen teknologiapinon tason tarpeiden mukaisesti. IoT-järjestelmän infrastruktuuria ja siihen liittyvää teknologiapinoa on kuvattu laajemmin aikaisemmassa luvussa 3.1, missä myös käydään läpi tätä kokonaisuutta tietoturvasuunnittelun kannalta. Tietoturvasuunnittelussa on otettava huomioon myös järjestelmässä sovellettavat pilvipalvelut, sekä niihin liittyvät tietoturvatekijät, joita on kuvattu laajemmin luvuissa 3.7, 4.1, 4.2 ja 4.4.

Kolmas ja samalla viimeinen tutkimuskysymys on: mikä on pk-yritysten ja esineiden internetin teknologia- ja tietoturvatilanne nyt? Tähän kysymykseen voidaan yhteenvetona vastata, että pk-yrityksille on Suomessa tarjolla tällä hetkellä paljon ulkoistettuja palveluita, jotka on tarkoitettu auttamaan esineiden internetiin liittyvien teknologioiden käyttöönotossa. Tarjottuihin palveluihin lukeutuu muun muassa erilaisia konsultaatiopalveluita ja ohjausta, valmiita- ja räätälöityjä IoT-ratkaisuja, ammattilaisten tuottamia tietoturvapalveluita ja ratkaisuja sekä erilaisia järjestelmän ylläpitoon liittyviä palveluita. Edeltävää on käyty läpi tarkemmin muun muassa luvuissa 4.2 ja 4.4. Palveluita ja uusia ratkaisuja kehitetään jatkuvasti lisää ja johtopäätöksenä tästä voidaan pitää, että kysyntää kyseisille ratkaisuille on olemassa kotimaisilla markkinoilla. Euroopan Unionin ja Suomen tahoilla toteutetaan kehitysyhteistyötä, minkä tuloksena pyritään tehostamaan esineiden internetin tietoturvaa ja luomaan uusia teknologisia ratkaisuja palvelemaan esineiden internetiä käyttävien yritysten erilaisia tarpeita. Edeltävästä on laajemmin kerrottu opinnäytetyön luvussa 4.5.

Tällä hetkellä pk-yrityksille on suunnattu kiitettävästi erilaisia ohjeistuksia, joiden kautta yritysten on mahdollista ymmärtää paremmin asioita, tehostaa yleistä tietoturvaa ja järjestelmäsuunnittelua sekä arvioida pilvipalveluita tarjoavien yhteistyöyritysten luotettavuutta ja tietoturvatasoa. Kyseisiä oppaita on saatavilla luotettavilta tahoilta, kuten Liikenne- ja viestintävirasto Traficomilta. Suoraa kattavaa ja yleistason opasta esineiden internetistä ei ole vielä saatavilla ainakaan Traficomilta tai vastaavilta tahoilta. Esineiden internet ja siihen liittyvät muut teknologiat ovat vielä kehittyvä kokonaisuus, joten tilanne niiden osalta muuttuu edelleen jatkuvasti. Edeltävästä on kerrottu laajemmin muun muassa tämän opinnäytetyön luvussa 4.2. Koska esineiden internet on vielä kehittyvä teknologia, tarkoittaa se myös sitä, että yhteiset standardit ovat vielä puutteellisia. Tämä tilanne paranee kuitenkin jatkuvasti ja standardointijärjestöt ovat aloittaneet erilaisia IoT-standardointihankkeita asiaan liittyen. Tällä hetkellä muun muassa IEEE-standardointijärjestö on hyväksynyt erittäin kattavan esineiden internetiä koskevan arkkitehtuurikehyksen. Kyseisen standardoinnin hyödyt kuitenkin konkretisoituvat pk-yrityksille vasta tulevaisuudessa. Standardointiin liittyvistä asioista on laajemmin kerrottu opinnäytetyön luvussa 3.4.

# 6 Pohdinta

Esineiden internet ja siihen liittyvät eri teknologiat muodostavat laajan kokonaisuuden, jonka hahmottaminen on välillä haasteellista. Kyseessä on kuitenkin edelleen kehittyvästä digitalisaatioon liittyvästä ilmiöstä, joka ei ole vielä saavuttanut täyttä kypsyyttä. Tästä johtuen dokumenttiaineiston kerääminen ja luotettujen kirjallisuuslähteiden löytäminen oli erittäin haastava ja aikaa vievä prosessi. Tämä edeltävä oli yllättävää ja työn edetessä käyttökelpoisten lähteiden löytäminen osoittautui hyvin työlääksi hakuprosessiksi ja myöhästytti työskentelyä useaan otteeseen. Tästä huolimatta varsinkin tietoperusta on työssä onnistunut, sillä siitä selviää paljon teknisiä asioita ja toisaalta myös yleistä käytännön tietoa, jota on mahdollista soveltaa myös käytännössä. Olen tyytyväinen myös työssä saavutettuihin tuloksiin ja empiiriseen osioon, sillä ne vastaavat opinnäytetyön alussa asetettuihin tutkimuskysymyksiin tarpeeksi kattavasti.

Projektina tämä työ on ollut haastava toteuttaa, mutta siitä on voitu oppia paljon. Muun muassa suunnittelutyön ja ajantasaisen dokumentaation ylläpitäminen ovat nousseet selvästi tärkeiksi asioiksi opinnäytetyön aihepiirin osalta. Tietoturvasuunnittelu täytyy yrityksissä toteuttaa ihan alkumetreiltä asti, kun otetaan käyttöön uusia järjestelmiä ja tämä on myös tosi esineiden internetin ratkaisujen kanssa. Resurssien ottaminen huomioon on myös keskeinen asia ja käytännössä tämä tarkoittaa sitä, että yrityksissä ei voi eikä pidä tehdä kaikkea yksin, jos parempi tulos on saavutettavissa ulkoistamalla kyseinen osa-alue ammattilaisille. Hyvän suunnittelun avulla voidaan minimoida riskejä ja ennaltaehkäistä tunnistettuja ja tunnistamattomia ongelmia, mikäli suunnitelmissa on otettu huomioon myös erilaiset poikkeustilanteet ja niistä toipuminen.

Kyseinen opinnäytetyö on kirjoittamisen hetkellä hyvin ajankohtainen, johtuen siitä, että esineiden internet on tällä hetkellä kehitysvaiheessa ja sen kysyntä on kasvanut Suomessa ja muualla maailmassa tasaisesti. Kyseinen teknologiasuuntaus kiinnostaa monia eri tahoja, mutta sen käyttöönottaminen on edelleen haasteellista. Näiden haasteiden takia markkinoille on ilmaantunut suuri joukko juuri pk-yrityksille suunnattuja palveluita, jotka pyrkivät tuomaan helpotusta esineiden internetin käyttöönotossa. Yleisenä suosituksena työn pohjalta voidaan todeta, että yritysten ja aiheesta kiinnostuneiden tahojen kannattaa aktiivisesti seurata esimerkiksi Traficomin julkaisuja, oppaita sekä uutisia liittyen kyseiseen aiheeseen ja tietoturvaan. Jatkuvasti kehittyvää tilannetta esineiden internetin kannalta voi myös tarkkailla palveluntarjoajien taholta ja yrityksille suunnattujen blogien ja uutissivustojen kautta. Näistä lähteistä saadut tuoreet tiedot voivat auttaa varsinkin päätöksentekoprosesseissa ja esimerkiksi hankintoja suunniteltaessa yrityksissä. Asiasta muu-

ten kiinnostuneita henkilöitä nämä lähteet voivat auttaa muilla tavoin ymmärtämään esineiden internetiä ja siihen liittyviä oheisteknologioita kokonaisuutena, josta voi olla hyötyä esimerkiksi työtehtävissä.

Tämä tutkimustyyppinen opinnäytetyö toteutettiin laadullisia menetelmiä käyttämällä ja sitä oli pyritty rajaamaan tarpeeksi helposti käsiteltäväksi kokonaisuudeksi. Työn toteuttamisen jälkeen on kuitenkin rajauksesta käynyt ilmi, että se olisi voitu toteuttaa vieläkin tiukemmilla raameilla, joka olisi sallinut yksittäisten asioiden tarkastelun syvällisemmin. Toisaalta toisenlainen lähestymistapa tässä työssä käsiteltyyn aiheeseen voisi myös olla toimiva ratkaisu. Eräänlainen kyselytutkimus, joka olisi rajattu koskemaan vaikkapa pääkaupunkiseudun pk-yrityksiä ja näiden yritysten käyttämiä esineiden internetin ratkaisuja olisi voinut myös tuottaa arvokasta tietoa tutkittavan aiheen kannalta. Tämä edeltävä voisi toimia hyvänä lähtökohtana tästä aiheesta jatkossa toteutettaville vastaaville opinnäytetöille ja tutkimuksille.

## Lähteet


Avast 2019. What risks do IoT security issues pose to businesses?. Luettavissa: https://blog.avast.com/iot-security-business-risk. Luettu: 17.3.2021.

Collin, J. & Saarelainen, A. 2016. Teollinen internet. Talentum. Helsinki. Luettavissa: https://haagahelia.finna.fi/Record/3amk.270261. Luettu: 11.2.2020.

Databros 2020. Pk-yrityksen tietoturvaopas. Databros. Seinäjoki. Luettavissa: https://www.databros.fi/content/uploads/Datagroup_databros_tietoturvaopas.pdf. Luettu: 28.2.2021.

DNA 2021a. Suojaa yrityksesi liiketoiminta kattavilla tietoturva-palveluilla. Luettavissa: https://www.dna.fi/yrityksille/tietoturva. Luettu: 18.4.2021.

DNA 2021b. Palomuuripalvelu suojaa yrityksesi verkon vaivattomasti. Luettavissa: https://www.dna.fi/yrityksille/tietoturva/palomuuri. Luettu: 18.4.2021.

DNA 2021c. Suojaa yrityksesi palvelunestohyökkäyksiä vastaan. Luettavissa: https://www.dna.fi/yrityksille/tietoturva/palvelunestohyokkayksilta-suojautuminen. Luettu: 18.4.2021.

DNA 2021d. Pääsynhallinnalla saat lujan otteen käyttöoikeuksista. Luettavissa: https://www.dna.fi/yrityksille/tietoturva/paasynhallinta. Luettu: 18.4.2021.

DNA 2021e. IoT - Esineiden internet. Luettavissa: https://www.dna.fi/yrityksille/iot. Luettu: 18.4.2021.

DNA Business 2020. 5G – kaikki mitä yrityspäättäjän pitää tietää. DNA Business. Helsinki. Luettavissa: https://uutiskirje.dna.fi/res/sibbe/DNA_WP_5G_kaikki_mita_pitaa_tietaa_e-kirja.pdf. Luettu: 10.2.2021.

Elisa Oyj 2021a. Verkon tietoturvapalvelut. Luettavissa: https://yrityksille.elisa.fi/tietoturva. Luettu: 18.4.2021.

Elisa Oyj 2021b. IoT - Esineiden Internet. Luettavissa: https://yrityksille.elisa.fi/iot. Luettu: 18.4.2021.

Euroopan Unionin julkaisutoimisto 2020. Käyttöopas Pk-yrityksen määritelmä. Euroopan Unionin julkaisutoimisto. Luxemburg. Luettavissa: https://op.europa.eu/s/omy8. Luettu: 22.10.2020.

IEEE Standards Association (IEEE SA) 2020. IEEE 2413-2019 - IEEE Standard for an Architectural Framework for the Internet of Things (IoT). Luettavissa: https://standards.ieee.org/standard/2413-2019.html. Luettu: 26.2.2021.

Ilmarinen, V. & Koskela, K. 2015. Digitalisaatio: yritysjohdon käsikirja. Talentum. Helsinki. Luettavissa: https://haagahelia.finna.fi/Record/3amk.210504. Luettu: 22.10.2020.

Industrial Internet Consortium 2015. Industrial Internet Reference Architecture. Industrial Internet Consortium. Milford, MA. Luettavissa: https://www.iiconsortium.org/IIRA-1-7-ajs.pdf. Luettu: 11.2.2021.

International Telecommunication Union (ITU) 2012. Recommendation ITU-T Y.2060 Overview of the Internet of things. International Telecommunication Union (ITU). Geneve. Luettavissa: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060. Luettu: 12.2.2021.

Kaspersky Lab 2017. What is Cyber Security?. Luettavissa: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. Luettu: 19.2.2021.

Kaspersky Lab s.a. Onko 5G-teknologia vaarallista? − 5G-verkon edut ja haittapuolet?. Luettavissa: https://www.kaspersky.fi/resource-center/threats/5g-pros-and-cons. Luettu: 16.3.2021.

LAMKpub 2019. Teollisten IoT-yhdyskäytävien rooli tiedon keräämisessä. Luettavissa: https://www.lamkpub.fi/2019/01/09/teollisten-iot-yhdyskaytavien-rooli-tiedon-keraamisessa/. Luettu: 16.3.2021.

Liikenne- ja viestintävirasto Traficom 2019. Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille. Liikenne- ja viestintävirasto Traficom. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf. Luettu: 17.4.2020.

Liikenne- ja viestintävirasto Traficom 2020. Pienyritysten kyberturvallisuusopas. Liikenne- ja viestintävirasto Traficom. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuus-opas_9_2020.pdf. Luettu: 18.3.2020.

Liikenne- ja viestintävirasto Traficom 2021. Ajankohtaista. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset. Luettu: 17.4.2020.

Mell, P. & Grace, T. 2011. The NIST Definition of Cloud Computing. The National Institute of Standards and Technology (NIST). Gaithersburg. Luettavissa: http://dx.doi.org/10.6028/NIST.SP.800-145. Luettu: 29.1.2021.

Mikrobitti 2020. Näin teollisuuden iot-järjestelmiin isketään – ”koko ajan yhä edistyneempiä hyökkäysvektoreita”. Luettavissa: https://www.mikrobitti.fi/uutiset/nain-teollisuuden-iot-jarjestelmiin-isketaan-koko-ajan-yha-edistyneempia-hyokkaysvektoreita/ac437742-96ae-4faa-a858-3ad8663b5d20. Luettu: 10.4.2021.

Mikrobitti 2021. Ei pelkkää pilveä – reunalaskenta kasvaa hurjaa kyytiä. Luettavissa: https://www.mikrobitti.fi/uutiset/ei-pelkkaa-pilvea-reunalaskenta-kasvaa-hurjaa-kyytia/7b100d8f-c825-4df1-8001-b9ade5a243c0. Luettu: 18.4.2021.

Neittaanmäki, P. & Siukonen, T. 2019. Mitä tulisi tietää tekoälystä. Docendo. Jyväskylä. Luettavissa: https://www.ellibslibrary.com/book/9789522916549. Luettu: 25.1.2021.

Shodan 2020. What is Shodan?. Luettavissa: https://help.shodan.io/the-basics/what-is-shodan. Luettu: 17.3.2021.

Suomen Yrittäjät, Finnvera Oyj, työ- ja elinkeinoministeriö 2020. Pk-yritysbarometri Kevät 2020. Suomen Yrittäjät ry. Helsinki. Luettavissa: https://www.yrittajat.fi/sites/default/files/sy_pk_barometri_kevat2020_2020.pdf. Luettu: 22.10.2020.

Telia Compan 2020. Näin yrityksesi voi hyödyntää reunalaskentaa. Luettavissa: https://www.telia.fi/yrityksille/artikkelit/artikkeli/nain-yritykset-voivat-hyodyntaa-reunalaskentaa. Luettu: 10.2.2021.

Telia Company 2021a. Tietoturva – kaikki ratkaisut. Luettavissa: https://www.telia.fi/yrityksille/infrapalvelut/tietoturva/kaikki-ratkaisut. Luettu: 18.4.2021.

Telia Company 2021b. IoT - Esineiden Internet. Luettavissa: https://www.telia.fi/yrityksille/iot/esineiden-internet. Luettu: 18.4.2021.

Telia Company 2021c. Asiantuntija-apua IoT:n kanssa. Luettavissa: https://www.telia.fi/yrityksille/iot/asiantuntijapalvelut?intcmp=b2b-palvelut-iot-ingressi-asiantuntijat. Luettu: 18.4.2021.

Telia Inmics-Nebula Oy 2018. Pilven monet kasvot – IaaS, PaaS ja SaaS. Luettavissa: https://www.inmicsnebula.fi/fi/blogi/pilven-monet-kasvot-iaas-paas-ja-saas. Luettu: 29.1.2021.

Tilastokeskus 2020. Pk-yritys. Luettavissa: https://www.stat.fi/meta/kas/pk_yritys.html. Luettu: 22.10.2020.

Työ- ja elinkeinoministeriö 2017. Suomen tekoälyaika – Suomi tekoälyn soveltamisen kärkimaaksi: Tavoite ja toimenpidesuositukset. Työ- ja elinkeinoministeriö. Helsinki. Luettavissa: http://urn.fi/URN:ISBN:978-952-327-248-4. Luettu: 20.12.2020.

Uusiteknologia 2018. Lokakuu 2/2018. Teknologiamediat Oy. Espoo. Luettavissa: https://www.uusiteknologia.fi/wp-content/uploads/2018/10/2_2018_low.pdf. Luettu: 25.2.2021.

Uusiteknologia 2020a. Verkkohyökkäysten riskit kasvussa – uhkaindeksi kertoo. Luettavissa: https://www.uusiteknologia.fi/2020/12/09/verkkohyokkaysten-riskit-kasvussa-indeksi-kertoo/. Luettu: 28.2.2021.

Uusiteknologia 2020b. Teollisuuteen uutta IoT-tekniikkaa ja tekoälyä. Luettavissa: https://www.uusiteknologia.fi/2020/06/23/teollisuuteen-uutta-iot-tekniikkaa-ja-tekoalya/. Luettu: 27.2.2021.

Uusiteknologia 2021a. Tuhat automaatiolaitetta suojaamatta – vaarassa myös IoT- ja etäyhteydet. Luettavissa: https://www.uusiteknologia.fi/2021/01/12/tuhat-automaatiolaitetta-edelleen-suojaamatta-vaarassa-myos-iot-ja-etayhteydet/. Luettu: 26.2.2021.

Uusiteknologia 2021b. Miksi uusin teknologia ei kiinnosta pk-yrityksiä?. Luettavissa: https://www.uusiteknologia.fi/2021/02/10/miksi-uusin-teknologia-ei-kiinnosta-pk-yrityksia/. Luettu: 26.2.2021.

Valtioneuvoston Selvitys- ja Tutkimustoiminta 2018. Lohkoketjuteknologian mahdollisuudet ja hyödyt sosiaali- ja terveydenhuollossa. Valtioneuvoston kanslia. Helsinki. Luettavissa: http://urn.fi/URN:ISBN:978-952-287-490-0. Luettu: 25.2.2021.

Valtiovarainministeriö 2009. VAHTI 7/2009 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä. Valtiovarainministeriö. Helsinki. Luettavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-72009-valtioneuvoston-periaatepaatos-valtionhallinnon-tietoturvallisuuden-kehittamisesta. Luettu: 28.1.2021.