

Benjami Junntila

**ÄLYKOTIEN VAKUUTTAMINEN
KYBERRISKEILTÄ– HAASTEET JA
MAHDOLLISUUDET VAKUUTUSYHTIÖIDEN
NÄKÖKULMASTA**

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Tammikuu 2023
Ohjaaja: Jarna Pasanen

TIIVISTELMÄ

Benjami Junttila: Älykotien vakuuttaminen kyberriskeiltä – haasteet ja mahdollisuudet vakuutusyhtiöiden näkökulmasta

Kandidaatintutkielma

Tampereen yliopisto

Kauppateiden tutkinto-ohjelma: Vakuutus ja riskienhallinta

Tammikuu 2023

Tässä tutkielmassa tarkastellaan älykoteihin liittyviä kyberriskejä sekä niiden vakuuttamisen haasteita ja mahdollisuuksia vakuutusyhtiöiden näkökulmasta. Tutkielmassa pyritään myös kartoittamaan, kuinka Suomessa toimivat vahinkovakuutusyhtiöt suhtautuvat älykotien kybervakuuttamiseen ilmiönä ja näkevätkö ne aiheen ajankohtaisena. Tutkimuskysymyksiä on yhteensä kaksi: (1) ”Millaisena ilmiönä vakuutusyhtiöt näkevät älykoteihin kohdistuvat kyberriskit ja niiden vakuuttamisen?” ja (2) ”Mitä haasteita ja mahdollisuuksia älykotien kybervakuuttamiseen liittyy?”.

Tutkielman teoriaosuudessa esitellään erikseen tausta- ja tulkintateoria omina päälukuinaan. Tutkielman taustateorian muodostavat kyberriskien ja kybervakuuttamisen teemat. Kyberriskien osalta keskitytään niiden luonteeseen, luokitteluun ja hallintaan. Kybervakuutusta tarkastellaan tuotteena ja lisäksi esitellään kyseisen vakuutuksen kattavuutta ja rajoituksia. Tutkielman tulkintateorian muodostavat IoT eli esineiden Internet ja älykodit. Esineiden Internetin osalta keskitytään sen luomiin mahdollisuuksiin ja haasteisiin sekä tulevaisuuteen. Älykotien taustoituksen jälkeen esitellään niiden laitteistoja ja järjestelmiä sekä perehdytään älykotien kyberriskeihin ja -turvallisuuteen.

Tutkielmassa hyödynnetään kvalitatiivisia eli laadullisia tutkimusmenetelmiä. Tutkielman aineisto kerättiin puolistrukturoidulla teemahaastattelulla ja haastatteluihin osallistui kolme asiantuntijaa kahdesta eri vahinkovakuutusyhtiöstä. Kerättyä aineistoa analysoidaan aineistolähtöisen sisällönanalyysin avulla, ja sen pohjalta tehdään johtopäätöksiä ja vastataan esitettyihin tutkimuskysymyksiin.

Tutkielman tuloksista käy ilmi, että näkemyksissä on hieman eroja eri vakuutusyhtiöiden edustajien välillä. Yleisesti ottaen älykotien ja kotitalouksien kyberriskit nähdään kuitenkin kasvavina ja jopa merkittävinä uhkina nyt ja tulevaisuudessa. Yleisimpien riskien osalta esiin nousivat identiteettivarkaudet ja muut henkilötietojen väärinkäytökset. Näille riskeille altistaviksi tekijöiksi esitettiin älylaitteiden heikkoa tietosuojaa sekä käyttäjän roolia. Älykotien kybervakuuttamisen osalta suurimpina haasteina nähtiin vakuutettavan ilmiön epämääräisyys, vahinkojen akkumulaatiopotentiaali, tuotteen hinnoittelu ja laitteiden standardien valvominen. Vakuuttajan näkökulmasta mahdollisuuksina nähtiin lisääntyvien riskien luoma tarve, älyteknologian hyödyntäminen proaktiivisessa riskienhallinnassa ja kasvava kysyntä ihmisten riskitietoisuuden lisääntyessä.

Avainsanat: älykoti, IoT, kyberriski, kybervakuutus

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

SISÄLLYSLUETTELO

1 JOHDANTO	1
1.1 Aihealueen esittely ja merkitys	1
1.2 Tutkielman tavoitteet, tutkimuskysymykset ja rajaukset.....	2
1.3 Tutkimusmenetelmät ja -aineistot.....	4
1.4 Keskeiset käsitteet.....	5
1.5 Tutkielman teoreettinen viitekehys ja rakenne	6
2 KYBERRISKIT JA -VAKUUTTAMINEN	8
2.1 Kyberriskit	8
2.1.1 Kyberriskin määritelmä ja luonne	8
2.1.2 Kyberriskien luokittelu.....	9
2.1.3 Kyberriskien hallinta	10
2.2 Kybervakuuttaminen.....	12
2.2.1 Kybervakuutus tuotteena.....	12
2.2.2 Kybervakuutusten kattavuus ja rajoitukset	13
3 IOT JA ÄLYKODIT ILMIÖNÄ	15
3.1 IoT eli esineiden Internet	15
3.1.1 IoT:n määrittely ja mahdollisuudet	15
3.1.2 IoT:n haasteet ja tulevaisuus	16
3.2 Älykoti	17
3.2.1 Älykotien tausta ja määrittely	17
3.2.2 Älykodin laitteet ja järjestelmät	18
3.2.3 Älykotien kyberriskit ja -turvallisuus.....	19
4 ÄLYKOTIEN KYBERVAKUUTTAMINEN	21
4.1 Aineiston kuvaus ja esittely	21
4.2 Kybervakuuttaminen nyt ja tulevaisuudessa.....	22
4.3 Yleisimmät kotitalouksiin kohdistuvat kyberriskit ja niiden vakuuttaminen ...	23
4.4 Älykotien kybervakuuttamisen haasteet ja mahdollisuudet.....	25
5 YHTEENVETO	28
5.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset.....	28
5.2 Tutkielman arviointi ja jatkotutkimusehdotuksia	29
LÄHDELUETTELO	31
LIITTEET	36
Liite 1 Haastattelurunko.....	36

KUVIO- JA TAULUKKOLUETTELO

Kuvio 1 Tutkielman teoreettinen viitekehys.....	6
Kuvio 2 Kyberriskien hallintakehikko.....	11
Kuvio 3 Älykoti-hankkeiden luokittelua suunniteltujen palveluiden mukaan.....	19
Taulukko 1 Älykotien kybervakuuttamisen haasteet ja mahdollisuudet	26

1 JOHDANTO

1.1 Aihealueen esittely ja merkitys

Älykodit ja niihin vahvasti linkittyvä IoT eli esineiden Internet ovat olleet kuumia ja kiinnostavia puheenaiheita viime vuosikymmenellä, kun uudet teknologiat ja innovaatiot ovat kehittyneet jättimäisin harppauksin. Esineiden ja asioiden langaton yhdistyminen Internetin kautta luo lukemattomia mahdollisuuksia ja käyttökohteita, mutta samalla myös lukuisia uusia riskejä sekä uhkakuvia (Geneiatakis, ym. 2017). Tästä seuraakin kysymys, että miten mahdollisilta kyberriskeiltä suojaudutaan älykotiratkaisujen yleistyessä ja voidaanko tällaisia riskejä siirtää esimerkiksi vakuutusten avulla. Yrityksille tarjottavat kybervakuutukset ovat jo arkipäivää vakuutusyhtiöille, mutta voisiko sama toimia myös kotitalouksien kohdalla?

Kyberhyökkäykset ja -rikollisuus ovat niin maailmalla kuin Suomessakin alati kasvava uhka (Traficom, 2022), joka tuskin tulee ainakaan vähentymään tulevaisuudessa. Kyberrikollisuuden uhrin voivat kokea monenlaisia haittoja, joista saattaa koitua suuriakin taloudellisia seuraamuksia. Esimerkiksi järjestelmien kaappaaminen, identiteettivarkaudet ja muiden arkaluontoisten tietojen vuotaminen voivat aiheuttaa kalliita ja aikaa vieviä selvitysprosesseja sekä suoria rahallisia menetyksiä. Toki kun puhutaan suurista kyberuhista ja -vuodoista, niin tarkoitetaan usein erilaisiin yrityksiin ja organisaatioihin kohdistuvaa rikollisuutta, mutta olisi tärkeä kuitenkin huomioida myös kotitalouksia ja yksityishenkilöitä koskeva kyberrikollisuus ja sen mahdolliset seuraukset.

Kybervakuuttamista on tutkittu yritystasolla jo pidemmän aikaa ja esimerkiksi Tampereen yliopistossa siitä on tehty useampikin opinnäytetyö, kuten Tia-Liisa Roikolan Pro gradu -tutkielma vuodelta 2017 ”Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa” sekä Kasimir Luostarisen kandidaatintutkielma vuodelta 2021 ”Kyberriskit ja niiden hallintaprosessi: Case Yritys Oyj”. Älykotien kyberriskeihin liittyvää tutkimusta on tehty huomattavasti vähemmän, mutta

kansainvälisesti aihealuetta ovat tutkineet muun muassa Arabo (2015) sekä Iten, Wagner & Zeier Röschmann (2021). Aihealuetta kartoittaessa löytyi myös yksi älykotipohjaisia vakuutuksia (Smart Home-Based Insurances) käsittelevä tutkimuspaperi, jonka avulla pyritään luomaan teoriaa ja ymmärrystä älykotien vakuuttamiseen (Eggert, 2019). Aiheen ajankohtaisuudesta ja mielenkiintoisuudesta kertoo osaltaan myös se, että maailmanlaajuinen aktuaarien ammatillinen järjestö Society of Actuaries on etsinyt vuonna 2022 tutkijoita tutkimaan älykotien kybervakuuttamiseen liittyviä teemoja (SOA, 2022).

Tämän tutkielman tarkoitus on ensisijaisesti paneutua älykotien vakuuttamiseen kyberriskeiltä, koska sitä ei ole juurikaan tieteellisesti tutkittu. Ulkomailta kuitenkin löytyy muutamia yhtiöitä, jotka tarjoavat tällaisia vakuutuksia useimmiten kotivakuutuksen lisäturvaksi (Residential Tech Today, 2020; Forbes, 2022). Näen siis aiheen tutkimisen merkittäväksi ja ajankohtaiseksi, koska tutkimusta löytyy niukasti, eikä Suomessa tällaisia vakuutus tuotteita ole tarjolla tällä hetkellä. Aihe on myös mielenkiintoinen niin vakuutusyhtiöiden kuin asiakkaidenkin näkökulmasta ja tulevaisuudessa ehkä jopa hyvinkin arkinen, kun erilaiset älykoti- ja IoT-ratkaisut yleistyvät yhä enemmän.

1.2 Tutkielman tavoitteet, tutkimuskysymykset ja rajaukset

Tutkielman tavoitteena on kartoittaa älykoteihin kohdistuvia kyberriskejä sekä niiden vakuuttamiseen liittyviä haasteita ja mahdollisuuksia Suomessa. Aihepiiriä tarkastellaan vakuutusyhtiön näkökulmasta, ja tarkoituksena onkin tuoda esille asiantuntijoiden näkemyksiä ja arvioita älykotien kybervakuuttamisesta ja -riskeistä. Näiden lisäksi tutkielma samalla kartoittaa onko aihe ylipäättään relevantti ja ajankohtainen vakuuttajien näkökulmasta. Tutkielma pyrkii ensisijaisesti vastaamaan seuraaviin tutkimuskysymyksiin:

1. Millaisena ilmiönä vakuutusyhtiöt näkevät älykoteihin kohdistuvat kyberriskit ja niiden vakuuttamisen?
2. Mitä haasteita ja mahdollisuuksia älykotien kybervakuuttamiseen liittyy?

Ensimmäisessä tutkimuskysymyksessä pureudutaan älykotien kyberriskeihin ja -vakuuttamiseen ilmiönä Suomessa toimivien vahinkovakuutusyhtiöiden näkökulmasta. Tutkimuskysymyksen avulla selvitetään, tunnistavatko vakuutusyhtiöt älykotiratkaisujen lisääntymiseen linkittyviä kyberriskejä, millaisia ne ovat luonteeltaan ja miten merkittävänä riskeinä ne koetaan nyt tai tulevaisuudessa. Jos älykoteihin kohdistuvia kyberriskejä pidetään merkittävänä riskeinä nyt tai tulevaisuudessa, selvitetään, onko niiden vakuuttaminen vakuutusyhtiöiden intressinä tällä hetkellä.

Toisen tutkimuskysymyksen tarkoituksena on kartoittaa vakuutusyhtiöiden näkemyksiä älykotien kybervakuuttamisen haasteista ja mahdollisuuksista. Tutkimuskysymyksen avulla kartoitetaan tekijöitä, jotka vaikuttavat kyseisen ilmiön vakuuttamiseen liittyviin haasteisiin. Lisäksi arvioidaan, voisiko näitä haasteita nähdä myös tulevaisuuden vahvuuksina tai mahdollisuuksina.

Tutkielma keskittyy ensisijaisesti kotitalouksien ja erityisesti älykotien vakuuttamiseen kyberriskeiltä. Tämä jättää siis syvällisemmän tarkastelun ulkopuolelle yrityksille tarjottavat kybervakuutukset sekä muut kotitalouksille suunnatut ennaltaehkäisevät kyberturvallisuuspalvelut, kuten erilaiset tietoturvaohjelmistot. Tästä huolimatta ennen kaikkea yrityksille suunnattuihin kybervakuutuksiin viitataan, jotta tutkittavaa ilmiötä saadaan pohjustettua ja taustoitettua riittävän kattavasti.

Toinen olennainen rajausta liittyy tutkielman näkökulman valitsemiseen, mikä on tuotu esille jo tutkielman otsikossa. Tutkimusilmiötä tarkastellaan Suomessa toimivien vahinkovakuutusyhtiöiden näkökulmasta, minkä voi perustella muutamallakin eri tavalla. Aiheen ollessa tuore ja melko vähän tutkittu niin luultavasti selkeimmät näkemykset ja asiantuntemus löytyy juuri suoraan vakuutusyhtiöistä. Kyseisen rajauksen oleellisuutta ohjaa myös tavoite selvittää kotitalouksille suunnattujen kybervakuutusten tuomista Suomen markkinoille.

1.3 Tutkimusmenetelmät ja -aineistot

Tässä tutkielmassa käytettiin kvalitatiivisia eli laadullisia menetelmiä, koska niiden avulla päästiin luontevammin käsiksi aihepiiriin ja pystyttiin löytämään vastaukset annettuihin tutkimuskysymyksiin. Tutkimustyyppiltään laadullista tutkimusta voidaan pitää empiirisenä, ja laadullinen tutkimus on vain eräänlainen empiirisen analyysin tapa argumentoida ja tarkastella havaintoaineistoa. Laadullista tutkimusta voidaan kutsua myös ymmärtäväksi tutkimukseksi, koska ilmiöitä voidaan joko yrittää ymmärtää tai selittää. (Sarajärvi & Tuomi, 2018, 21–25.) Tässä tutkielmassa tutkimusilmiötä pyritään ensisijaisesti ymmärtämään ja kuvailemaan, koska aihe on tuore ja vähän tutkittu.

Kun tehdään asianmukaista ja laadukasta tutkimusta, oli se sitten kvalitatiivista tai kvantitatiivista, niin ei sovi unohtaa teorian merkitystä. Laadulliseen tutkimukseen sovelletaan kahdenlaista eri teoriaa, jotka ovat tausta- sekä tulkintateoria. Taustateoriaa tarvitaan, jotta tutkimusaineistoa voidaan tarkastella sitä vasten. Sen sijaan tulkintateoria ohjaa tutkijaa etsimään aineistosta vastaukset haluttuihin kysymyksiin. Vahvan teorian luominen auttaa tutkielman teossa ja sitä voi jopa pitää eräänlaisena tutkielman ajatuspohjana. (Eskola & Suoranta, 1998.)

Tutkimusaineiston kerääminen empiiristä osiota varten toteutettiin puolistrukturoituna haastatteluina eli teemahaastatteluina, joille on tyypillistä etukäteen valitut teemat ja kysymykset (Sarajärvi & Tuomi, 2018, 65). Haastattelun kysymykset ja eteneminen oli ennalta määritelty, mutta haastateltavat saivat vastata kysymyksiin täysin avoimesti. Haastatteluihin saatiin kolme vakuutusyhtiön edustajaa kahdesta eri Suomessa toimivasta vakuutusyhtiöstä. Haastateltavilta löytyi asiantuntemusta sekä kyber- että kotivakuuttamisesta, mikä loi osaltaan syvyyttä aiheen tarkasteluun ja näkökulmiin.

Kerätyn aineiston analysointi suoritettiin aineistolähtöisenä sisällönanalyysina. Pääpiirteissään siihen kuuluu aineiston kirjoittaminen puhtaaksi, pelkistäminen, luokittelu ja eri luokkien yhdistely eheäksi kokonaisuudeksi (Sarajärvi & Tuomi 2018, 91–94). Analyysin pohjalta tehtiin lopuksi yhteenvetoa sekä johtopäätöksiä, ja pohdittiin vastauksia tutkielmalle asetettuihin tutkimuskysymyksiin. Tässä tutkielmassa oman

pohdinnan ja reflektoinnin osuus kasvoi lopulta aika merkittäväksi aiheen luonteen ja sen pohjalta käytyjen haastatteluiden vuoksi.

1.4 Keskeiset käsitteet

Tämän alaluvun tarkoituksena on avata muutamia keskeisiä käsitteitä tutkielma kannalta, jotta lukijalla on tarvittava ymmärrys käsiteltävästä aiheesta. Käsitteiden määrittely tarkoittaa myös sen, mitä niillä tarkoitetaan kyseisessä tutkielmassa. Keskeisten käsitteiden määrittely auttaa myös empiirisen osion ja siitä saatujen tulosten omaksumisessa.

Kyberriskit ovat erilaisiin tieto- ja hallintajärjestelmiin kohdistuvia uhkia, jotka voivat aiheuttaa laajoja sekä moninaisia vahinkoja. Kyberriskejä voidaan luokitella eri muuttujien kuten tahallisuuden, hyökkäystyyppin ja tekijöiden mukaan. Suurin osa kyberriskeistä koostuu kuitenkin tahallisista kyberhyökkäyksistä, joissa rikolliset pyrkivät esimerkiksi kiristämään rahaa kaappaamalla järjestelmiä tai tietoja itselleen. (Eling & Schnell, 2016.) Tämä tutkielma tarkastelee kyberriskejä ja niiden realisoitumisen seurauksia lähtökohtaisesti kotitalouksien näkökulmasta, mutta teoriapohja koostuu pitkälti yrityksiin kohdistuvista kyberuhista.

Kybervakuutus on vakuutus, jolla pyritään siirtämään kyberriskien realisoitumisesta koituvat kustannukset vakuutusyhtiölle. Kybervakuutukset ovat tällä hetkellä lähinnä yrityksille tarjottavia palveluita, jotka voidaan muokata yksilöllisten tarpeiden mukaan ja vakuutus voi yhdistellä useampaa eri vakuutuslajia keskenään. Kybervakuutuksella voidaan sopimuksen mukaan korvata useita erilaisia vahinkoja kuten liiketoiminnan keskeytymisestä tai kyberhyökkäyksestä ja sen selvittelystä aiheutuneita kuluja. (Aon, 2022.) Vaikka kybervakuutus käsitteenä liittyy vahvasti yritysvaluuttamiseen niin tässä tutkielmassa sitä käytetään yleisemmällä tasolla kattaen näin myös mahdolliset älykoodille suunnatut kybervakuutukset.

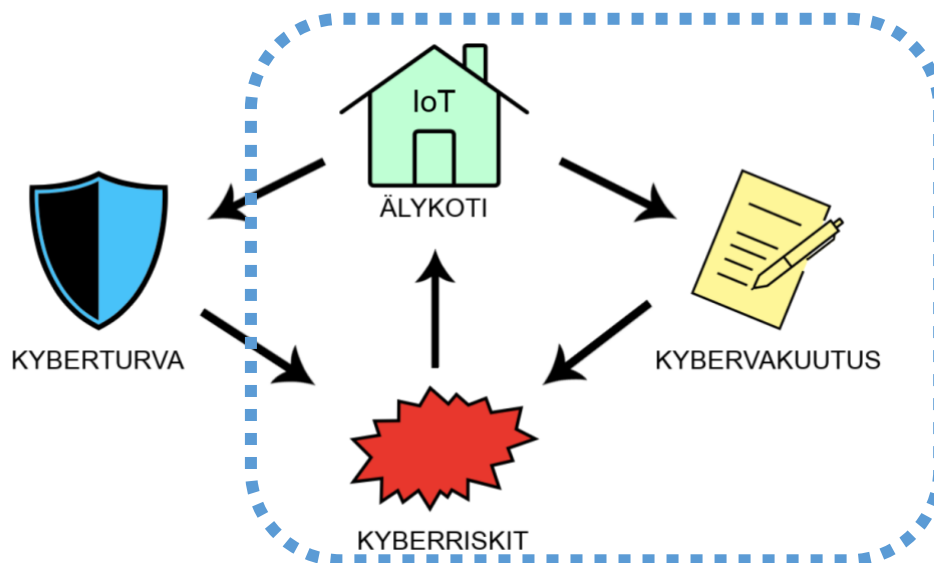
IoT (Internet of Things) eli esineiden Internet on järjestelmä, jossa eri laitteet ja ohjelmat ovat yhteydessä toisiinsa ja hallittavissa langattoman verkon välityksellä. Tämä mahdollistaa osaltaan asioiden automatisoinnin ja laitteiden etäohjauksen, mikä linkittyy

samalla vahvasti älykotiympäristön luomiseen. (Pătru, Carabaş, Bărbulescu, & Gheorghe, 2016.) Tässä tutkielmassa keskitytään nimenomaisesti kotien IoT-järjestelmiin ja niiden haavoittuvuuksiin, mutta systeemien syvällisempi ymmärtäminen ei ole keskiössä.

Älykodilla tarkoitetaan tässä tutkielmassa kotia, johon on integroitu laitteita tai palveluita hallitsemaan kodin eri järjestelmiä sekä parantamaan asukkaiden elämänlaatua. Älykoteknologia liittyy usein esimerkiksi kodin turvallisuuteen, lämmitysjärjestelmään ja laitteiden etäohjaukseen erilaisten langattomien yhteyksien kautta. (Mocrii, Chen & Musilek, 2018.) Termi voidaan määritellä monella eri tavalla, mutta tässä tutkielmassa määritelmä pidetään suhteellisen avoimena, koska täysin automatisoituja ja ”älykkäitä” koteja on loppupeleissä hyvin vähän olemassa. Myöskään näiden älyteknologioiden ja niihin liittyvien riskien vakuuttaminen ei ole vakiintunut, joten aiheen käsittely on mielekkäämpää laajemman määritelmän kautta.

1.5 Tutkielman teoreettinen viitekehys ja rakenne

Tässä aluvuossa esitellään ja taustoitetaan tutkielman teoreettinen viitekehys sekä käydään läpi tutkielman rakenne aina johdannosta yhteenvetoon asti. Teoreettisen viitekehysten tarkoituksena on auttaa lukijaa orientoitumaan tutkielman teoriaosuuteen ja antaa yleiskatsaus aihepiiristä, jota tutkielma käsittelee. Rakenteen esittely kuvaa lyhyesti tutkielman etenemisen pääotsikkotasolla, mikä auttaa hahmottamaan tutkielman etenemistä. Alla oleva Kuvio 1 havainnollistaa tutkielman teoreettisen viitekehksen.



Kuvio 1 Tutkielman teoreettinen viitekehys

Tutkielman teoreettinen viitekehys (Kuvio 1) kuvaa visuaalisesti yksinkertaistetussa muodossa tutkielmassa esiteltävät teoriaosuudet ja niiden väliset vuorovaikutussuhteet. Viitekehysten pääkomponentteina ovat IoT-teknologiaan pohjautuva älykoti, kybervakuutus, kyberriskit sekä kyberturva. Tutkielman teoriapohja ja aihepiiri kytkeytyvät asetelman ympärille, jossa IoT-järjestelmiä hyödyntävään älykotiin kohdistuu kyberriski, jonka realisoituessa aiheutuneita vahinkoja voitaisiin korvata kybervakuutuksen avulla. Kyberturva on luonnollisesti olennainen osa älykotien ennakoivaa suojausta ajatellen ja siksi se myös kuviossa esiintyy. Älykotien kyberturvallisuus ei ole kuitenkaan tutkielman asetelman vuoksi keskiössä eikä sitä varsinaisesti käsitellä teoriaosuudessa pääotsikkotasolla, minkä vuoksi se on jätetty katkoviivalla merkityn laatikon ulkopuolelle.

Tutkielman rakenne koostuu pääpiirteittäin johdannosta, tausta- ja tulkintateoriaosuudesta sekä tutkimustulosten esittelystä, analysoinnista ja yhteenvedosta. Tutkielman johdanto-osio päättyy tähän kyseiseen rakenteen esittelyyn, jota seuraa ensimmäinen teoriaosuus. Luvun 2 taustateorian tarkoituksena on pohjustaa tutkimusaihetta ja siinä käydään läpi kyberriskeihin sekä kybervakuuttamiseen liittyviä teemoja. Kolmannessa luvussa paneudutaan tulkintateoriaan, jonka aiheina ovat esineiden Internet ja älykodit sekä näihin liittyvät ilmiöt. Tämän jälkeen neljännessä luvussa siirrytään kerätyn haastatteluaineiston esittelemiseen ja analysointiin. Viimeisessä eli viidennessä luvussa vastataan tutkimuskysymyksiin, luodaan koostava yhteenveto, arvioidaan tutkimuksen laatua ja luotettavuutta sekä tehdään katsaus tulevaisuuden jatkotutkimusmahdollisuuksiin. Aivan lopuksi on vielä lueteltu tutkielmassa käytetyt lähteet sekä liitetiedostot.

2 KYBERRISKIT JA -VAKUUTTAMINEN

2.1 Kyberriskit

2.1.1 Kyberriskin määritelmä ja luonne

Kyberriskit on viime vuosina luokiteltu maailmanlaajuisesti suurimmaksi yrityksiä koskevaksi riskilajiksi, mikä näkyy myös vuoden 2022 riskibarometrissä (Allianz, 2022). Kyberriskejä on myös viime vuosikymmeninä tutkittu jatkuvasti enemmän, mutta yhtä vakiintunutta määritelmää sille ei ole silti muodostunut. Käsitettä käytetään laajasti eri tieteenaloilla kuten tietotekniikassa, liikkeenjohdossa ja yhteiskuntatieteissä. (Strupczewski, 2021.) Kyberriskin määrittelyyn vaikuttaa varmasti osaltaan myös niiden kompleksisuus ja moniulotteisuus. Böhme, Laube & Riek (2019) esittelevät kybervahingoille kolme luokittelevaa asetelmaa, jotka ovat kyberuhan vaikutus kyberkohteeseen, fyysisen uhan vaikutus kyberkohteeseen sekä kyberuhan vaikutus fyysiseen kohteeseen.

Hieman suoraviivaisempaa lähestymistapaa kyberriskin määritelmäksi tarjoavat Mukhopadhyay, ym. (2013), joiden mukaan kyberriski määritellään riskiksi, joka liittyy haitalliseen sähköiseen tapahtumaan, josta aiheutuu liiketoiminnan häiriöitä ja rahallisia menetyksiä. Tästä vieläkin karsitumman näkemyksen ovat jo vuonna 2003 julkaistussa artikkelissaan esittäneet Gordon, Loeb & Sohail, joiden mukaan kyberriski on Internetiin pohjautuva riski. Tämän voi ajatella olleen aikanaan ihan yleispätevä määritelmä, mutta toki nykytiedon ja -teknologian valossa erittäin suppea sekä epämääräinen ilmaisu.

Suhteellisen kattavan määritelmän mukaan kyberriskin käsite pitää sisällään kaikki riskit, jotka johtuvat sähköisen tiedon käytöstä ja sen välittämisestä, mukaan lukien teknologiset välineet, kuten Internet ja televerkot. Riski kattaa myös verkkohyökkäysten aiheuttamat fyysiset vahingot, tietojen väärinkäytöstä johtuvat petokset, tietojen säilytyksestä johtuvat vastuut sekä sähköisen tiedon saatavuuden, eheyden ja luottamuksellisuuden. Kyberriski voi näin ollen myös kohdistua joko yksityishenkilöihin, yrityksiin tai

kokonaisuun valtioihin. (CRO Forum, 2014.) Tämä kuvaus antaa hyvää osviittaa kyberriskien luonteesta, mutta jo edellä esiteltyjen määritelmien pohjalta voidaan luontevasti todeta, ettei kysymykseen ole vain yhtä oikeaa vastausta.

2.1.2 Kyberriskien luokittelu

Kyberriskeistä puhuttaessa tulee usein ensimmäisenä mieleen erilaiset kyberhyökkäykset ja muu rikollinen toiminta, mikä on toki ymmärrettävää, koska suurista tietoturvaluotoista ja -hyökkäyksistä usein myös uutisoidaan enemmän. Sen lisäksi rikollistarkoituksessa tehdyt kyberiskut ovat usein niitä yleisimpiä kyberriskejä. Tästä huolimatta kyberriskejä voidaan jaotella tahallisiin ja tahattomiin. Tahallisiksi kyberriskeiksi voidaan luokitella esimerkiksi erilaiset hakkerien tekemät kyberiskut. Sen sijaan tahaton kyberriski voi tulla kyseeseen esimerkiksi tilanteessa, jossa arkaluontoista dataa jaetaan alustalle, johon on asiaankuulumattomilla tahoilla vapaa pääsy. (Refsdal, Solhaug & Stølen, 2015, 34.)

Yleisimpiä kyberhyökkäystyyppisiä ovat verkkourkinta (phishing), erilaiset haittaohjelmat (malware), käyttäjien manipulointi (social engineering) ja palvelunestohyökkäykset (DDoS) (Sobers, 2022). Verkkourkinta on hyvin yleinen hyökkäystyyppi, joka voidaan lukea osaksi käyttäjien manipulointia. Siinä rikollinen pyrkii kalastelemaan kohteeltaan henkilökohtaisia ja arkaluontoisia tietoja esimerkiksi väärennetyjen sähköpostien ja verkkosivujen avulla. (Gupta, Singhal & Kapoor, 2016.) Erilaisia haittaohjelmia on lukemattomia määriä ja niitä kehitetään jatkuvasti lisää. Yhdeksi suurimmista yritystoimintaa häiritseviksi haittaohjelmatyypiksi voisi nostaa erilaiset kiristyshaittaohjelmat (ransomware). Kiristyshaittaohjelmien ydinajatuksena on, että ohjelma rajoittaa käyttäjän pääsyä elintärkeisiin tietoihin ja vaatii rajoituksen purkamista vastaan jonkinlaista maksua uhrilta. (Brewer, 2016.) Palvelunestohyökkäyksillä pyritään usein lamauttamaan esimerkiksi jonkin yrityksen verkkosivusto kohdistamalla siihen niin paljon liikennettä, että sen palvelin ylikuormittuu. Tämänkaltaiset hyökkäykset ovat Internetissä hyvin tyypillinen ja vakava ongelma, mutta yleensä niiden tarkoitus ei ole kuitenkaan vahingoittaa tietoja suoraan tai pysyvästi. (Douligeris & Mitrokotsa, 2004.)

Maailman suurin jälleenvakuutusyhtiö Munich Re nostaa vuoden 2022 kyselyraportissaan kolme yleisintä kyberuhkien aiheuttajaa yrityksissä. Nämä ovat

yleisyyden mukaan järjestyksessä verkkopetokset eli verkkourkinta, tietomurrot sekä kiristyshaittaohjelmat. Kaikki edellä mainitut uhkatekijät olivat nousseet 7–11 prosenttiyksikkö vuodesta 2021 ja tutkimuksen mukaan jopa yli 71 % kyselyyn vastanneista yrityksistä oli jo kärsinyt kiristysohjelmista tai verkkohyökkäyksestä, joka on aiheuttanut petoksia tai tietomurtoja. (Munich Re, 2022.) Kyberriskit ovat monesti hyvin salakavalia uhkia, jotka täytyy tosissaan ottaa huomioon yritystoiminnassa, mutta suurin osa riskeistä voidaan eliminoida hyvin suunnitelluilla ja toteutetuilla hallintakeinoilla.

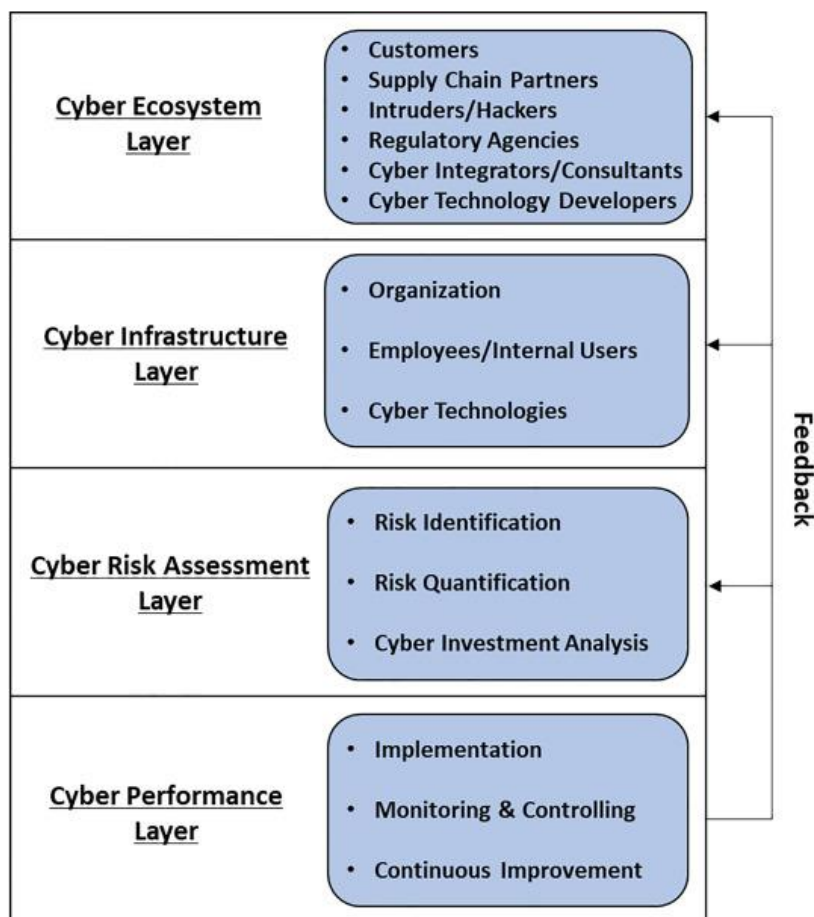
2.1.3 Kyberriskien hallinta

Kyberriskien hallinta lähtee liikkeelle samankaltaisista peruspalikoista kuin yritysten perinteinen riskienhallintaprosessi, mutta kyberriskien luonne muokkaa toki pitkälti lähestymistapoja hallintakeinoihin. Suomen Riskienhallintayhdistys (2022) jakaa riskienhallintaprosessin neljään päävaiheeseen, jotka ovat riskien tunnistaminen ja arviointi, riskienhallintakeinot, varautuminen vahinkoihin sekä seuranta ja vahingoista oppiminen. Tällainen runko on oikein toimiva ja hyvä perusmuotti mistä lähteä koko yrityksen riskienhallintaa toteuttamaan, mutta perehdytään seuraavaksi siihen, miten yrityksen tai organisaation kyberriskejä voidaan lähteä hallitsemaan.

Organisaatioissa kyberriskien hallitseminen on usein keskittynyt tietoturvaohjelmistojen kehittämiseen, järjestelmien suunnitteluun ja parhaiden toimintatapojen löytämiseen sekä osaavaan työvoiman investoimiseen tietoturvan saralla. Kyberhyökkäyksiltä voidaan suojautua monilla eri mekanismeilla kuten palomureilla, ohjelmistojen salauksella, virustunnistuksella ja järjestelmän lokeroinnilla. (Paté-Cornell, Kuypers, Smith & Keller, 2018.) Nämä edellä mainitut suojauskeinot ovat ennakoivia toimenpiteitä, joilla pyritään estää hyökkääjää pääsemästä käsiksi yrityksen tiedostoihin ja järjestelmiin. Samoin myös henkilöstön kouluttamisella ja fiksuilla toimintatavoilla voidaan parantaa yrityksen kyberpuolustusta sisältäpäin.

Kokonaisvaltaisemmin kyberriskien hallintaa lähtee kartoittamaan Lee (2021) artikkelissaan, joka käsittelee riskienhallintaa ja investointikustannusten analyysia kyberturvallisuuden näkökulmasta. Lee (2021) on luonut oman kyberriskien hallintakehikon, joka jakautuu neljään eri tasoon. Nämä tasot ovat kyberekosysteemi

(Cyber Ecosystem Layer), kyberinfrastruktuuri (Cyber Infrastructure Layer), kyberriskien arviointi (Cyber Risk Assessment Layer) ja kybertoiminnan suorituskyky (Cyber Performance Layer). Seuraavaksi Kuvio 2 esittää edellä mainitun hallintakehikon.



Kuvio 2 Kyberriskien hallintakehikko (Lee, 2021, Fig. 1, 662)

Leen (2021) koostamassa kuviossa kyberekosysteemi on päällimmäinen taso ja siihen kuuluvat erilaiset sidosryhmät, jotka ovat osana yrityksen tietoverkkoja sekä -liikennettä. Tämä korostaa sitä, kuinka olennaisessa roolissa yrityksen kanssa toimivat tahot ovat kyberturvallisuuden luomisessa ja miksi ne pitää tunnistaa. Kyberinfrastruktuuri on sen sijaan taso, jossa tarkastellaan yrityksen sisäisiä toimintoja, joilla suojaudutaan kyberriskeiltä. Tämä taso keskittyy kyberriskien hallinnassa nykyiseen teknologiaan, ihmisen käytökseen sekä organisaation toimintatapoihin ja strategiaan. Kolmas taso eli kyberriskien arviointi pureutuu kolmeen osa-alueeseen, jotka ovat riskien tunnistaminen, riskien kvantifiointi eli määrittäminen valitun suureen avulla sekä kyberinvestointien analysointi. Lopulta kybertoiminnan suorituskykyä tarkastellaan viimeisellä tasolla toteutuksen, valvonnan ja kontrolloinnin sekä jatkuvan kehittymisen näkökulmista.

Neljännän tason on tarkoitus asettaa tavoitteita ja seurata säännöllisesti muiden tasojen toimintaa ja palautteen avulla pyrkiä kehittämään yrityksen kyberriskien hallintaa sekä strategisia suuntaviivoja.

2.2 Kybervakuuttaminen

2.2.1 Kybervakuutus tuotteena

Kyber- tai tietoturvakvakuutus on vakuutusluku, jolla suojaudutaan kyberriskien realisoiutumisesta seuranneilta vahingoilta, kuten tietomurron aiheuttamilta kustannuksilta (Peters, Shevchenko, & Cohen, 2018, 11). Hieman toisin sanoin kybervakuuttamista tutkimuksessaan kuvaavat Böhme & Schwartz (2010). Heidän mukaansa kybervakuuttaminen on verkko- ja tietokonevahinkojen siirtämistä kolmannelle osapuolelle eli tässä tapauksessa vakuutusyhtiölle. Molemmat määritelmät ovat toimivia ja kuvaavat hyvin kybervakuutusten luonnetta. Kybervakuuttaminen on ollut suuren murroksen ja kehityksen kohteena viime vuosikymmeninä, kun kyberriskejä on alettu paremmin ymmärtämään ja tunnistamaan. Silti vielä suhteellisen uudehkona vakuutusluku kybervakuutusluku markkinat kohtaavat edelleenkin kehittyessään täysin uudenlaisia haasteita. (Marotta, ym., 2017.) Parhaassa tapauksessa kybervakuutukset parantavat yrityksen ennakoivaa riskienhallintaa, kun riskeihin sekä suojausmekanismeihin kiinnitetään enemmän huomiota. Pahimmillaan riskienhallinta jää vakuutuksen myötä staattiseksi ja yrityksen kannalta epäoptimaaliselle tasolle, jolloin puolustuksessa keskitytään ennaltaehkäisyyn sijasta reaktiiviseen torjuntaan. (Shackelford, 2012.)

Ensimmäiset kybervakuutusluku tuotteet voidaan ajoittaa 1990-luvun lopulle, kun AIG tarjosi ensimmäistä Internetin turvallisuusvastuuvakuutusta keväällä 1997. Erään määritelmän mukaan kyberturva voidaan jakaa kolmeen osa-alueeseen, jotka ovat kolmannen ja ensimmäisen osapuolen suojaus sekä niin sanottu hiljainen kybersuoja. (Granato & Polacek, 2019.) Tässä yhteydessä kolmannella osapuolella tarkoitetaan muun muassa vakuutusluku ottajien asiakkaita ja esimerkiksi heidän tietojen vuotamisesta johtuneita vahinkoja. Ensimmäisellä osapuolella tarkoitetaan itse vakuutusluku ottajaa eli yritystä ja sen mukaan korvauksia maksetaan suoraan yrityksen liiketoimintaan vaikuttavien

kustannusten kattamiseksi. Hiljaisella kyberturvalla viitataan tässä vahinkoihin, jotka korvataan normaalista omaisuus- ja vahinkovakuutuksesta, vaikka vahingon alkuperän voitaisiin osoittaa johtuneen oikeastaan kyberhyökkäyksestä. (Granato & Polacek, 2019.) Esimerkkinä korvauksia voidaan maksaa yrityksen omaisuusvakuutuksesta, jos yrityksen tietojärjestelmien kaappaaminen aiheuttaa tapahtumaketjun, jonka seurauksena joitakin laitteistoja vahingoittuu. Toki tällaiset tapahtumat vaativat aina kokonaisvaltaista arviointia sekä voimassa olevien vakuutusten ja niiden ehtojen tulkitsemista.

2.2.2 Kybervakuutusten kattavuus ja rajoitukset

Kybervakuutukset kuten kaikkia muutkin vakuutukset ovat pohjimmiltaan vain kaksipuolisia sopimuksia, joita koskee luonnollisesti erilaiset ehdot ja rajoitukset. Tästä syystä on olennaista käydä läpi hieman korvattavia ja ei korvattavia vahinkoja sekä yleisimpiä rajoituksia, joita Suomessa tarjottaviin kybervakuutuksiin on liitetty. Suomessa toimivista vahinkovakuutusyhtiöistä kyber-/tietoturvakvakuutusta tarjoavat ainakin kaikki Suomen suurimmat vahinkovakuuttajat (Finanssiala, 2021), jotka ovat Pohjola Vakuutus, LähiTapiola-ryhmä, If Vahinkovakuutus Oyj (Suomen sivuliike), Fennia ja Turva.

Tarkastellaan seuraavaksi hieman neljän suurimman vahinkovakuuttajan (Pohjola Vakuutus, LähiTapiola, If ja Fennia) kybervakuutusten kattavuutta ja niihin liittyviä rajoituksia. Kaikkiin neljään sisältyy itse kybervakuutuksen ohella 24/7 puhelinpalvelu, josta saa kellon ympäri apua kyberhyökkäysten varalle, jolloin suojaus ja turvatoimet voidaan aloittaa välittömästi. Yleisimpiä kybervakuutuksesta korvattavia vahinkoja ovat tietomurron selvittämiseen, hoitamiseen ja tietojen palauttamiseen liittyvät kustannukset, liiketoiminnan keskeytymisestä johtuvat kustannukset sekä kolmansille osapuolille aiheutuneet taloudelliset vahingot. Korvauksen piiriin kuuluvat usein myös erilaiset maineenhallintaan liittyvät kustannukset ja esimerkiksi pakollisesta tiedonantovelvollisuudesta aiheutuneet kustannukset. (Fennia, 2022; If, 2022; LähiTapiola, 2022; Pohjola Vakuutus, 2022.)

Yleisimpiä ja selkeästi ei korvattavia vahinkotyypppejä ovat henkilö- ja esinevahingot sekä sakot ja muut rangaistusluonteiset maksut kuten sopimusrikkomukset. Erilaiset rajoitusehdot ja niiden noudattaminen vaikuttaa myös oleellisesti siihen korvataanko

jokin vahinko vakuutuksesta vaiko ei. Kybervakuutuksien rajoitukset koskevat pitkälti yrityksen tietoturvaan liittyviä turvatoimia kuten tietojen päivittäinen varmuuskopiointi, tietojärjestelmien ja ohjelmistojen ylläpito sekä kyberturvan pitäminen ajan tasalla. Myös esimerkiksi yrityksen kirjanpidon on oltava kunnossa, jos keskeytysvakuutuksesta aikoo korvauksia saada. (Fennia, 2022; If, 2022; LähiTapiola, 2022; Pohjola Vakuutus, 2022.) Toki kybervakuutuksia koskee yhtä lailla muutkin yleiset rajoitusehdot kuten sodat, ympäristökatastrofit ja vilpillinen menettely. Tässä alaluvussa käsiteltiin vain yleisimpiä kybervakuutuksiin liittyviä korvauskäytäntöjä ja rajoituksia eikä kuvaus ole siis kaiken kattava. Tarkemmat tiedot ja kuvaukset löytyvät erikseen kunkin vakuutusyhtiön vakuutusehdoista.

3 IOT JA ÄLYKODIT ILMIÖNÄ

3.1 IoT eli esineiden Internet

3.1.1 IoT:n määrittely ja mahdollisuudet

IoT eli esineiden Internet on tunnistettu yhdeksi tulevaisuuden tärkeimmistä osa-alueista teknologian saralla ja sen hyödyntämistä pyritään jatkuvasti kehittämään useilla eri aloilla. Esineiden Internetin tarkoitus on luoda koneiden ja laitteiden välinen yhteys, jonka kautta ne pystyvät toimimaan vuorovaikutuksessa keskenään. IoT:n luoma lisäarvo yrityksille saadaan täysimääräisesti hyödynnettyä silloin kun siihen liitetyt laitteet kykenevät saumattomasti kommunikoidaan keskenään ja integroitumaan yrityksen käyttämiin järjestelmiin, sovelluksiin ja analytiikkaan. (Lee & Lee, 2015.)

Esineiden Internetin käsitettä ja tutkimusta tarkastelevat Sorri, Mustafee & Seppänen (2022) artikkelissaan, jossa he systemaattisen kirjallisuuskatsauksen sekä temaattisen analyysin avulla luokittelevat IoT:n määritelmiä. Nelivaiheisen prosessin päätteeksi he luokittelevat IoT:n määritelmät kymmeneen eri kategoriaan. Kategorioiksi valikoituvat lopulta *Interaction*, *Virtual Thing*, *Services*, *Physical Object*, *Standardised Technologies*, *Information*, *Data*, *Ubiquitous*, *User* ja *Unique*. Seuraavassa kappaleessa luetellut kategoriat avataan lyhyesti artikkelin määritelmien mukaan.

Interaction tarkoittaa, että virtuaaliset laitteet ovat yhteydessä toisiinsa ja kykenevät vuorovaikuttamaan keskenään. *Virtual Thing* on aktiivinen laite, joka kerää ja mahdollisesti tallentaa fyysisen esineen toimintaan liittyvät tiedot. *Services* tarkoittaa järjestelmän toimintoja jonkin prosessin parantamiseksi. *Physical Object* on yksinkertaisesti esine, johon virtuaalinen asia upotetaan. Se voi olla myös esine, jonka suorituskykyä valvotaan. *Standardised Technologies* viittaa keinoihin, jotka mahdollistavat tiedonkeruun. *Information* kuvaa tässä yhteydessä tietojenkäsittelyä. *Data* tarkoittaa todellisia bittejä ja tavuja kuten raakadataa ja big dataa. *Ubiquitous* kuvaa sitä, että tietojen on oltava saatavilla missä tahansa, mutta ei välttämättä kaikkialla. *User*

tarkoittaa ihmisen ja koneen välistä vuorovaikutusta. *Unique* määrittäyty sillä, että kaikki esineet ja asiat on yksilöitävä tiedonkeruuta ja analysointia varten. (Sorri, Mustafee & Seppänen, 2022.) Kaiken kaikkiaan artikkelista käy siis selkeästi ilmi, että IoT:n määritelmät vaihtelevat hyvin suuresti ja samalla tutkimus aiheen ympärillä on kasvanut runsaasti viime vuosien aikana. Artikkelissa todetaan myös esineiden Internetin mahdollistavan organisaatioille uusia liiketoimintamahdollisuuksia tietoon perustuvan muutoksen avulla.

Esineiden Internetin käyttömahdollisuudet eivät suinkaan rajoitu pelkästään yritysmaailmaan, vaan teknologioita sovelletaan paljon myös kuluttajien tarpeisiin. Tästä esimerkkeinä erilaiset älykellot, älyvalot ja jopa älyhammasharjat (Figueiredo e Silva, Kaseva & Lohan, 2018). IoT on hyvin olennainen osa koko älykotikonseptia ja siksi sen luomien mahdollisuuksien tunnistaminen on tutkielman kannalta relevanttia. Mocrii, Chen & Musilek (2018) kuvaavat, ettei IoT ole vain joukko toisiinsa yhdistettyjä laitteita ja sensoreita, vaan se on virtuaalimaailman ja todellisuuden muodostama integraatio, jossa ihmisten ja laitteiden välinen kommunikaatio tapahtuu.

3.1.2 IoT:n haasteet ja tulevaisuus

Esineiden Internetiin liittyy suurien mahdollisuuksien lisäksi myös luonnollisesti paljon erilaisia haasteita ja uhkakuvia, niin kuin uusille innovaatioille sekä teknologian kehitykselle on usein tapana. Esineiden Internetin uhiksi voidaan luetella muun muassa verkon haasteet, turvallisuus, viansietokyky, käyttöjärjestelmien kehitys sekä uusien ja monitahoisten riippuvuuksien haasteet. Verkon haasteet liittyvät erilaisten laitteiden ja järjestelmien sovittamiseen yhdeksi keskenään kommunikoivaksi kokonaisuudeksi. Siihen kytkeytyy myös laitteiden energiantarve, minkä optimointi on hyvin tärkeää uusien elektroniikkalaitteiden lisääntyessä. Turvallisuus ja laitteiden tietoturva ovat ehdottoman olennainen osa esineiden Internetiä ja haasteena onkin, miten laitteet pystytään suojaamaan niin, ettei arkaluontoisi tietoja pääse väärin käsiin. IoT-järjestelmien viansietokyky pääsee koetukselle, kun ohjelmistoissa tapahtuu virheitä, joita tietokone ei pysty ratkomaan. Laitteiden ja sensoreiden keräämän datan määrä kasvaa jatkuvalla tahdilla, minkä vuoksi käyttöjärjestelmien tulisi pysyä kehityksessä mukana ja prosessoimaan lisääntyviä tietomassoja. (Farhan, ym. 2017.)

Edelliseen tutkimukseen verrattuna samankaltaisia uhkia ovat artikkelissaan nostaneet esille Karie, Sahri & Haskell-Dowland (2020). He nostavat IoT:n merkittävimmiksi uhiksi nykyaikana yksityisyyteen, turvallisuuteen, yhdenmukaisuuteen, integraatioon, liitettävyyteen ja regulaatioon liittyvät haasteet. Samainen artikkeli nostaa esille myös neljä tulevaisuuden kehityssuuntaa esineiden Internetin näkökulmasta. Ensimmäisenä näkemyksenä nostetaan IoT-laitteiden potentiaali muuttaa monia päätöksentekotilanteita tekoälyn, koneoppimisen ja syväoppimisen avulla. Esineiden Internetin perusheikkoutena on nähty laitteiden lisääntyneen tietoturvan hallinta ja toisena kehitysaskelena mainitaan reunalaskennan (Edge Computing) hyödyntäminen, joka nopeuttaisi IoT-laitteiden tiedonkäsittelyä. Kolmantena kehityskohteena nähdään lohkoketjuteknologian integroiminen osaksi esineiden Internetiä, jolloin verkon välityksellä hoidetut transaktiot sujuisivat entistä turvallisemmin. Viimeisenä, muttei suinkaan vähäisimpänä mainitaan tutkimus- ja kehitystyön lisääminen turvallisuuden parantamiseksi, koska se tulisi asettaa etusijalle. (Karie, ym. 2020.)

3.2 Älykoti

3.2.1 Älykotien tausta ja määrittely

Älykoti voidaan määritellä monella eri tavalla ja ajatuksen juuret sijoittuvat jopa niinkin kauas kuin 1930-luvulle saakka, jolloin esiteltiin ensimmäisiä visioita tulevaisuuden kodeista. Tästä huolimatta lupaukset ”ennennäkemättömästä ylellisyydestä, rentoutumisesta ja hemmottelusta” sekä ”nykyaikaisen elämisen eduista vähemmällä vaivannäöllä” alkoivat toteutumaan vasta vuosisadan viimeisillä kymmenillä. (Mocrii, Chen & Musilek, 2018.) Tiedettävästi ensimmäisenä termin ”älytalo” otti virallisesti käyttöön American Association of House Builders vuonna 1984, tarkoituksenaan edistää tarvittavan teknologian sisällyttämistä uusien asuntojen suunnitteluun (Harper, 2003; Dingli & Seychell, 2015).

Vuonna 2004 julkaistussa artikkelissa Jiang, Liu & Yang määrittelevät älykkään kodin sisältävän ainakin kolme elementtiä, jotka ovat sisäverkko, älykäs ohjaus ja kodin automaatio. Sen sijaan näkökulmaa älykotien ensisijaisista tavoitteista tarjoaa Suresh & Sruthi vuonna 2015 julkaistussa kirjallisuuskatsauksessaan. Heidän mukaansa älykotien

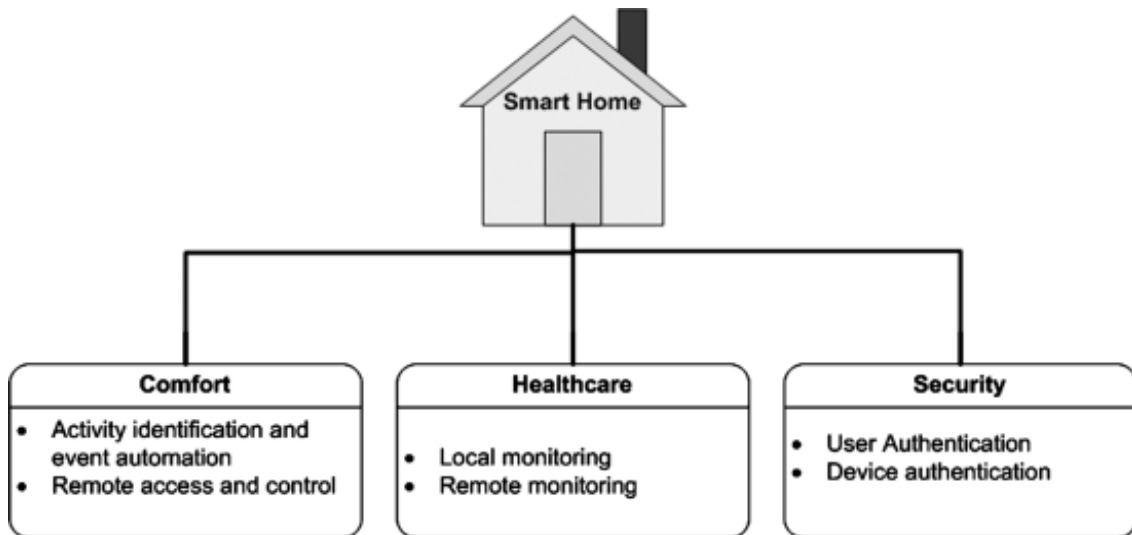
tärkeimmät tehtävät ovat helpottaa ihmisten tavanomaista elämää, minimoida energiankulutusta sekä tukea iäkkäiden ja vammaisten omavaraisuutta.

Älykkään kodin teknologiaa voisi kuvailla järjestelmäksi, joka kaikkea ympäröivää tietotekniikkaa hyödyntäen yhdistää älykkyyden ja automatisaation kotiympäristöön mukavuutta, valvontaa, turvallisuutta, terveydenhoitoa ja energiansäästöä varten (Alam, Reaz, & Ali, 2012). Ehkä hieman yksinkertaisemmin termiä määrittelevät Iten, Wagner & Zeier Röschmann vuonna 2021 julkaistussa artikkelissaan. Heidän määritelmänsä mukaan älykoti on varustettu älykkäillä teknologioilla, jotka tarjoavat asukkaalle etä-, digi- ja automatisoituja palveluita, joiden tarkoitus on parantaa kotielämän laatua. Yhteenvetona voisi todeta, että älykotitekniikat pyrkivät pääosin parantamaan sekä helpottamaan ihmisten arkea, mutta täysin yksiselitteistä määritelmää ei älykodille ole vielä vakiintunut. Tätä voisi selittää osaltaan uusien teknologioiden vauhdikas ja jatkuva kehitys sekä aihepiirin monimuotoisuus ja -tulkinnallisuus.

3.2.2 Älykodin laitteet ja järjestelmät

Kuten jo aikaisemmin on käynyt ilmi niin älykodeissa oleellisena osana ovat erilaiset elämänlaatua parantavat älylaitteet, sensorit ja järjestelmät. Näiden älyteknologioiden avulla voidaan esimerkiksi lisätä kodin automaatiota, helpottaa energianhallintaa ja vähentää ympäristöpäästöjä (Saad al-sumaiti, Ahmed & Salama, 2014). Useita kodin älylaitteita voidaan ohjata ja seurata puhelimeen asennettavien applikaatioiden välityksellä ja yleisiä toimintoja ovat muun muassa kodin valaistuksen, lämmityksen sekä lukituksen hallinta. Myös erilaiset älytelevisiot ja muut etäohjattavat kodin viihdelaitteet ovat yleistyneet kuluttajien keskuudessa. (Pättru, ym. 2016.)

Tutkimuksessaan Alam, Reaz, & Ali (2012) jaottelevat älykotihankkeet kolmeen eri kategoriaan, jotka muodostuvat tutkijoiden kiinnostuksen sekä käyttäjien vaatimusten ja odotusten mukaan. Kategoriat on jaoteltu mukavuuteen, terveydenhuoltoon ja turvallisuuteen. Seuraavaksi Kuvio 3 esittelee älykotihankkeiden luokittelua suunniteltujen palveluiden mukaan.



Kuvio 3 Älykotihankkeiden luokittelua suunniteltujen palveluiden mukaan (Alam, Reaz, & Ali, 2012, Fig. 1, 1191)

Ensinnäkin mukavuuden ja helppouden maksimointi on ehdoitta yksi älykotien pääteemoista ja se voidaan saavuttaa kahdella eri tavalla. Mukavuuden lisääminen perustuu ihmisen toiminnan tunnistamiseen ja toimintojen automatisointiin sekä kodin etäohjaukseen. Toisekseen älykotiratkaisuilla on mahdollista parantaa terveydenhuoltoa niin vanhusten, sairaiden kuin terveidenkin osalta. Tämä perustuu paikalliseen ja etäseurantaan eli älykotiympäristö voisi tunnistaa terveydentilan muutoksia ja varoittaa niistä paikallisesti asukkaalle sekä mahdollisissa hätätapauksissa, kuten sairaskohtauksissa, ilmoittaa ongelmista suoraan terveydenhuollon ammattilaisille. Kolmanneksi osa-alueeksi kuviossa on nostettu turvallisuus ja yksityisyydensuoja, jotka tulevat väistämättä esille, kun älykodeista puhutaan. Useimmat ongelmat turvallisuuden suhteen liittyvät heikkoon todentamiseen käyttäjien sekä laitteiden osalta, jolloin näihin tulisi kiinnittää suurta huomiota. (Alam, Reaz, & Ali, 2012.)

3.2.3 Älykotien kyberriskit ja -turvallisuus

Teknologiset järjestelmät ja edistysaskeleet tuovat usein mukanaan uusia riskejä ja sama pätee myös älykotitekniologioiden kohdalla. Uusien innovaatioiden kuten IoT:n, tekoälyn, pilvilaskennan ja yhä laajemman sensoritekniikan käyttöönotto on tehnyt älykodeista entistä käytännöllisempiä, mutta samalla myös todella houkuttelevia kohteita kyberhyökkäyksille. Suurin osa älylaitteisiin ja järjestelmiin kohdistuvista kyberriskeistä ei sinällään ole kyseisellä kentällä uusia, mutta niiden yhdistäminen kotioloihin luo

ennenkokemattomia uhkia asukkaiden fyysiseen sekä henkiseen turvallisuuteen. (Heartfield, ym. 2018.)

Artikkelissaan Abdullah, ym. (2019) nostavat älykotien suurimmiksi haavoittuvuustekijöiksi heterogeeniset järjestelmät, vanhentuneet käyttöliittymät, heikot salaukset, rajoittuneet tallennustilat ja prosessorit, epävarmat sovellukset, huonon tunnistautumisen sekä laiteohjelmistoviat. Rikolliset ja muut pahantekijät voivat hyödyntää näitä haavoittuvuuksia ja täten luoda monenlaisia uhkia. Näitä uhkia ovat muun muassa erilaiset palvelunestohyökkäykset (DoS), salakuuntelu, tietojen kalastelu ja varastaminen, arkaluontoisten tietojen paljastaminen sekä erilaisten haitta- ja vakoiluohjelmien asentaminen. Aiheutetut vahingot voivat siis olla hyvinkin dramaattisia ja konkreettisia yksilön kannalta, minkä vuoksi kyberturvallisuus olisi syytä ottaa tosissaan huomioon älyteknologiaa hyödyntävien kotitalouksien osalta.

Älykotien kyberturvaa voidaan vahvistaa monilla eri keinoilla, mutta keskeisiä suojaustoimia ovat ainakin asianmukaiset ja ajantasaiset käyttöjärjestelmät vahva käyttäjän tunnistautuminen sekä asukkaiden tietoturvatietoisuuden lisääminen. Vahvaa tunnistautumista voitaisiin konkretisoida erilaisilla biometrisillä tunnisteilla kuten, sormenjälki- tai iiristunnistuksella. Suojatun langattoman yhteyden (WLAN/Wi-Fi) käyttäminen estää hyökkääjiä kaappaamasta verkkoyhteyttä ja näin vähentää mahdollisuutta päästä käsiksi arkaluontoisiin tietoihin. Suojattujen viestintäyhteyksien ylläpitäminen sekä käytön rajoittaminen vain valtuutetuille käyttäjille vähentää laitteiden manipulointiin liittyviä riskejä ja näin ollen myös taloudellisia tappioita. (Ali & Awad, 2018.) Tosiasia on kuitenkin se, että vaikka kuinka huolellisesti riskeihin osaisi valmistautua niin lähes aina jää joitakin riskejä kannettavaksi. Tämän vuoksi on asianmukaista pohtia, voitaisiinko osa älykotien kyberriskeistä siirtää pois itseltä vakuutusten avulla.

4 ÄLYKOTIEN KYBERVAKUUTTAMINEN

4.1 Aineiston kuvaus ja esittely

Tutkielman aineistot kerättiin puolistrukturoituina teemahaastatteluina loka-marraskuun aikana. Haastatteluita varten oltiin syksyn aikana yhteydessä useaan Suomessa toimivaan vahinkovakuutusyhtiöön ja lopulta haastatteluihin osallistui kolme asiantuntijaa kahdesta eri vahinkovakuutusyhtiöstä. Ensimmäinen haastattelu suoritettiin parihaastatteluna, mikä nähtiin tutkimustavoitetta edistäväksi, koska samasta yhtiöstä saatiin kaksi eri tehtävissä toimivaa edustajaa. Toinen haastattelu oli perinteinen yksilöhaastattelu toisen yhtiön edustajan kanssa. Molemmat haastattelut suoritettiin etäyhteyksin ja haastattelurungot lähetettiin asianomaisille jo ennen haastattelujen suorittamista, jotta niihin sai rauhassa tutustua etukäteen. Sen lisäksi haastattelut nauhoitettiin litteroinnin helpottamiseksi. Kaikilta haastateltavilta pyydettiin lupa haastatteluiden nauhoittamiseen ja henkilötietojen käsittelyssä noudatettiin EU:n yleistä tietosuojaa-asetusta (2016/679). Tutkielmasta on jätetty suorat tunnistetiedot mainitsematta niin yhtiöiden kuin niiden edustajienkin osalta, koska yhtiö- ja henkilötietojen esiintuominen ei ole tutkielman ja sen tulosten kannalta merkityksellistä. Selkeyden vuoksi sekä hahmottamisen helpottamiseksi haastateltavista käytetään tarpeen mukaan termejä A, B ja C. Näistä A sekä B edustavat Yhtiötä 1 ja C edustaa Yhtiötä 2.

Ensimmäisestä yhtiöstä haastateltava A toimii yritysten omaisuuden ja toiminnan vakuutusten kehityspäällikkönä ja tuoteomistajana, minkä kautta asiantuntemusta löytyy myös yritysten kybervakuuttamisen puolelta. Samaisesta yhtiöstä haastateltava B toimii kehityspäällikkönä koti- ja venevakuutuksissa sekä on kodin henkilö- ja omaisuusvahinkojen tuoteomistaja. Tämän pohjalta tietotaitoa ja näkökulmia tarjoutui kotivakuutusten puolelta. Haastateltava C on puolestaan toisen yhtiön edustaja ja toimii siellä johtotehtävissä suuryritysten digitaalisten riskien ja kyberpalveluiden parissa. Häneltä saatiin asiantuntevaa näkemystä kyberturvallisuudesta ja -vakuuttamisesta.

Haastatteluissa käytetty haastattelurunko löytyy kokonaisuudessaan tutkielman lopusta (Liite 1). Haastattelurunkoon sisältyi yhteensä 13 kysymystä ja se on jaoteltu taustakysymysten lisäksi kolmeen eri teemaan. Ensimmäinen teema liittyy pääasiassa kybervakuuttamiseen tällä hetkellä ja kysymyksillä pyrittiin saamaan yleiskuvaa yhtiöiden tarjoamista kybervakuutustuotteista. Tämän teeman yhteydessä sivuttiin myös hieman kybervakuuttamisen mahdollisia tulevaisuuden suuntaviivoja. Toisen teeman tarkoituksena oli kartoittaa kotitalouksien kyberriskejä ja niiden hallintaa ja pohtia älyteknologian lisääntymisen vaikutusta riskeihin. Kolmannessa teemassa paneuduttiin älykotien kybervakuuttamiseen sekä siihen liittyviin haasteisiin ja mahdollisuuksiin. Lopussa oli myös mahdollisuus nostaa muita mielenkiintoisia näkökulmia tai teemoja esiin. Tulokset esitellään seuraavissa luvuissa teemoittain pääfokuksen ollessa älykotien kyberriskeissä ja -vakuuttamisessa.

4.2 Kybervakuuttaminen nyt ja tulevaisuudessa

Haastattelun ensimmäisessä teemassa käsiteltiin siis kybervakuuttamista tällä hetkellä ja molemmista yhtiöistä nousi suhteellisen samankaltaisia asioita esiin, mikä oli toki myös odotettavissa. Molemmilla yhtiöillä on omat kybervakuutustuotteensa pk-yrityksille, mutta ehkä olennaisimpana erona on, että Yritys 1 tarjoaa isommille asiakkaille kybervakuutuksia yhteistyökumppaninsa kautta, kun taas Yritys 2 tarjoaa omaa kybervakuutustaan suurasiakkailleen, mikä on samantyyppinen kuin muilla kansainvälisillä kilpailijoilla.

Kummallakin yhtiöllä kybervakuutukset korvaavat vakuutetuille itselleen sattuvia vahinkoja ja niiden hoitamiseen liittyviä kuluja kuten it-tuki ja konsultointi. Tämän lisäksi pääkohdiksi kybervakuutuksiin liittyen nostettiin vastuu- ja keskeytysvahingot, joista C nosti jälkimmäisen kenties keskeisimmäksi turvaksi, koska yritykset ovat ehkä eniten huolissaan siitä nykypäivänä. Haastateltava C:n mukaan yrityksiin kohdistuvista kyberuhista tällä hetkellä yleisimpiä ovat kiristyshaittaohjelmat (ransomware), jonka lisäksi myös tietomurrot ja -varkaudet ovat keskeinen uhka. Kommentit tukevat siis hyvin aikaisemmin tutkielmassa käsiteltyä taustateoriaa.

Kybervakuutuksen ohella A mainitsi heillä olevan käytössä 24/7 puhelinpalvelu, johon voi ottaa yhteyttä kyberturvaan liittyen. Tämän lisäksi Yhtiö 1 tarjoaa muita tietoturvapalveluita asiakashintaan yhteistyökumppanin kautta ja erillinen tietoturvaa käsittelevä pdf-koulutusmateriaali on saatavilla. Lisäpalveluista C kommentoi vain suuryritysten osalta ja niihin kuului tyypillisesti riski-insinöörien hyödyntäminen pienissä tietoturvakartoituksissa ja konsultoinnissa. Tämän lisäksi tarjolla on eräänlainen kolmannen osapuolen riskikartoitus, joka tuottaa uhkatietoa kohdeyrityksen ympäristöstä ja antaa dataa ikään kuin hakkerin näkökulmasta. Lisäpalveluna tällaisia tietoturvaraportteja voidaan tarjota noin muutaman kerran vuodessa.

Kybervakuutusten lähimenneisyydestä ja -tulevaisuudesta tuli hieman eriäväisiä näkemyksiä haastatteluiden kesken, sillä A:n mielestä kybervakuutustuotteet eivät ole juurikaan muuttuneet alkuaajoista, mutta C:n mukaan kybervakuutusmarkkinassa on viimeisen kahden vuoden sisällä tapahtunut merkittävä kiristyminen hintojen ja tarjonnan osalta. Tämän näkemyseron voi luultavasti selittää yksinkertaisesti sillä, että kysymykseen on lähdetty hakemaan vastausta hieman eri näkökulmista. Molemmissa puheenvuoroissa tulee kuitenkin ilmi, ettei kybervakuutus ole vielä ihan täysin valmis tuote ja se hakee edelleen paikkaansa. Haastateltava C kuitenkin korosti, että oman näkemyksensä mukaan markkinapenetraatio tulee kasvamaan rajusti yrityspuolella vielä jatkossa ja kybervakuutus tulee olemaan suuri sekä merkittävä tuote 10 vuoden päästä sekä ylipäättään tulevaisuudessa. Kotitalouksien osalta haastateltava B mainitsi, että kyberriskien aiheuttamat omaisuusvahingot ovat vielä melko tuntemattomia tällä hetkellä, jonka vuoksi tilastoja ja dataa ole saatavilla. Hän myös totesi kyberrikollisuuden keskittyvän enemmän yrityksiin, koska kotitalouksista on vähemmän taloudellista rikoshyötyä saatavilla, mikä on toki hyvin loogista.

4.3 Yleisimmät kotitalouksiin kohdistuvat kyberriskit ja niiden vakuuttaminen

Haastattelujen pohjalta kotitalouksiin ja yksityishenkilöihin kohdistuvista kyberriskeistä korostuivat selkeästi identiteettivarkaudet ja muu henkilötietojen väärinkäyttö. Molemmissa keskusteluissa nousi esille myös, että identiteettivarkauksille altistaa luonnollisesti yhä enemmän se, että lähes kaikki asioiminen ja liikenne tapahtuu nykyisin

verkon välityksellä ja tietokoneiden avustuksella. Tässä kohdassa vastaukset olivat jokseenkin odotusten mukaisia, mutta kummassakaan haastattelussa ei nostettu konkreettisenä uhkana esille arkaluontoisten tietojen kalasteluun liittyvää verkkourkintaa (phishing) ja sen eri alalajeja. Tämä tuntuu olevan kuitenkin erittäin yleinen ilmiö nykypäivänä jo pelkästään uutisten ja omakohtaisten kokemusten perusteella.

Kaikki haastateltavat nostivat esille laitteiden heikon tietoturvan merkityksen, kun mietitään, mikä kotitalouksia altistaa eniten kyberriskeille. Kotitalouksien heikkoon tietoturvaan ja riskien kasvamiseen löytyi ainakin kolme selkeää tekijää, jotka ovat laitemäärien jatkuva kasvu, laitteiden huono tietoturva ja käyttäjän rooli. Laitemäärien kasvu on jo itsessään riskejä nostava tekijä, kun erilaiset datapisteet ja iskukohtat lisääntyvät. Sekä A, että C nostivat halvalla tuotettujen laitteiden tietoturvan merkittäväksi riskitekijäksi. Samassa yhteydessä C kuitenkin muistutti, ettei tietoturvaan aina panosteta niin antaumuksella myöskään suurten länsimaisten tuotemerkkien kohdalla, kun tarkoituksena on myydä massoittain laitteita suurella kätteellä. Käyttäjän roolin merkitystä korosti haastateltava B esimerkiksi salasanojen hallinnan kautta. Haastateltava C antoi riskien muodostumisessa suuren painoarvon kotitalouksien heikolle kybersuojalle ja tietoturvaosaamiselle verrattuna yritysmaailmaan. Esille nousi myös älylaitteiden päivittämisen tärkeys, mikä on luonnollisesti käyttäjän vastuulla. Näiden lisäksi C esitti mielenkiintoisen ilmiön koskien etätyön lisääntymistä, jonka myötä useat yritysten tietokoneet pyörivät nyt ihmisten kotiverkoissa samojen huonosti suojattujen ja päivittämättömien laitteiden kanssa. Täten voisi ajatella, että osa kotitalouksiin kohdistuvista kyberriskeistä on siirtynyt nyt myös yrityksille.

Toisen teeman lopussa oleva kysymys sai osakseen hieman eriäviä mielipiteitä, koskien älykotiteknologian yleistymiseen liittyvien kyberriskien merkittävyttä kotitalouksille nyt tai tulevaisuudessa. Haastateltava C:n mielestä älykotiteknologian yleistyminen on todella iso riski kotitalouksille nyt ja paljon suurempi riski tulevaisuudessa. Sen sijaan haastateltava B kommentoi riskin olevan varmasti kasvava tällä hetkellä, kun laitteet yleistyvät, mutta ei pidä sitä valtavana ja merkittävänä riskinä kotitalouksille. Haastateltava B kylläkin tunnisti riskit henkilötietoihin ja identiteettivarkauksiin liittyen, mutta aika näyttää onko vielä hieman teorian tasolla olevat fyysiset laitteisiin kohdistuvat riskit todellisia tulevaisuudessa.

Älykotien kybervakuuttamisen yhteydessä nousi B:n puheenvuorossa taas esille se vakuutusyhtiön näkökulmasta ongelmallinen asia, että dataa ja esimerkkitapauksia ei ole oikein vielä saatavilla. Tästä huolimatta sekä B, että C nostivat esille, että esimerkiksi identiteettivarkauksien ja nettikiusaamisen varalle on jo olemassa joitakin vakuutusturvia, jotka ovat usein liitetty osaksi kotivakuutusta. Kummallakaan yhtiöllä ei ollut tällä hetkellä suoraan yksityishenkilöille tai kotitalouksille tarjottavia kybervakuutuksia, mutta kybervakuutuksenomaisia piirteitä sisältyy osaksi joihinkin heidän kotivakuutustuotteisiinsa. Mielenkiintoisena huomiona voisi nostaa, että Yhtiössä 1 on taannoin kokeiltu eräänlaista älykotivakuutusta, mutta sen myynti lopetettiin kokeilujakson jälkeen. Haastateltava B myös kertoi, että samaisessa yhtiössä on käytössä älyvalvontaa hyödyntävä vesivuotovahti pientaloihin. Se ei suoranaisesti liity kybervakuuttamiseen, mutta siinä on hieman samoja elementtejä älyteknologiaan ja ennakoivaan reagoimiseen liittyen. Tällaiset vahinkoja ehkäisevät innovaatiot ovat hyödyksi vakuutetulle sekä vakuuttajalle ja ne voivat luoda suuriakin säästöjä verrattain pienellä investoinnilla.

4.4 Älykotien kybervakuuttamisen haasteet ja mahdollisuudet

Älykotien kybervakuuttamisen haasteisiin ja mahdollisuuksiin tuli hieman erilaisia näkemyksiä, mikä luultavasti johtuu osittain taas siitä, että vastauksia lähdettiin purkamaan erilaisista kulmista. Tarkastellaan ensin älykotien kybervakuuttamiseen liittyviä haasteita ja edetään siitä kohti mahdollisuuksia. Haastateltava B nosti esille, että suoranaisesti kotiin kohdistuvat kyberriskit ovat vielä aika teoreettisella tasolla ja ei oikein vielä osata sanoa mikä se vakuutettava riski ylipäättään on. Tämä ilmiön epämääräisyys tekee vakuuttamisen näkökulmasta asian melko ongelmalliseksi.

Haastateltava C kiinnitti huomiota ilmiöön linkittyvään akkumulaatiopotentiaaliin, mikä on todella iso riski ja haaste vakuuttajan näkökulmasta. Tästä esimerkkinä oli, että millaisia vastuuta siitä voisi seurata, jos jotakin laitetta on myyty kymmeniä miljoonia kappaleita ympäri maailman ja siitä löydetään merkittävä haavoittuvuus, jota voidaan tehokkaasti hyödyntämään rikollisten toimesta. Tämän lisäksi C mainitsi myös, että hinnoittelua vaikeuttaa epätietoisuus älylaitteiden määrästä kodeissa, mikä vaikuttaa

suoraan riskitasoon. Sääntelyn perspektiivistä haasteita liittyy laitteiden standardien valvomiseen, kun laitteita voi tilata mistä vain ilman varmuutta niiden turvallisuudesta.

Mahdollisuuksien osalta haastateltava A nosti esille ihmisten ikääntymisen riskinä kybermaailmassa. Se saattaisi alkaa luomaan painetta vakuuttamiselle, jos aletaan huomaamaan, että esimerkiksi ikääntyvälle väestölle alkaa sattua enemmän vahinkoja. Haastateltava C lähestyi asiaa uhkakuvan kautta eli siellä missä on uhka, on myös mahdollisuus. Hänen mielestään älylaitteisiin ja esineiden Internetiä hyödyntävään teknologiaan liittyvä kyberuhka luo mahdollisuuksia samalla kybervakuuttamiseen. Tässäkin yhteydessä nousi jälleen kerran esille kodin älylaitteiden heikko tietoturva. Haastateltava B korosti puheenvuorossaan ehkä enemmän erilaisten älyteknologioiden hyödyntämistä vakuuttamisessa. Hän kertoi älyteknologian tuoneen paljon mahdollisuuksia esimerkiksi vahinkojen vähentämiseen ja muuhun proaktiiviseen toimintaan vahinkojen ehkäisyyn liittyen. Älykotilaitteiden hyödyntäminen voi tuoda myös paljon lisää vahinkopuolen ja korvausten sujuvuuteen tulevaisuudessa. Lopuksi B mainitsee myös kysynnän kasvaneen etenkin identiteettivarkauksien osalta. Seuraavaksi Tauluko 1 kokoaa älykotien kybervakuuttamisen haasteisiin ja mahdollisuuksiin liittyviä havaintoja yhteen.

Taulukko 1 Älykotien kybervakuuttamisen haasteet ja mahdollisuudet

ÄLYKOTIEN KYBERVAKUUTTAMINEN	
HAASTEET	MAHDOLLISUUDET
Vakuutettavan ilmiön ja konkreettisten riskien epämääräisyys	Ihmisten ikääntymisen luoma tarve uusille vakuutustuotteille
Vahinkojen akkumulaatiopotentiaalinen riski vakuuttajalle	Lisääntyvät kyberuhat luovat mahdollisuuden vakuuttamiselle
Älylaitteiden määrän vaikutus tuotteiden hinnoitteluun	Älyteknologian hyödyntäminen ja proaktiivinen riskienhallinta
Sääntelyn haasteet laitteiden standardien valvomisessa	Kasvava kysyntä ihmisten riskitietoisuuden lisääntyessä

Tästä päästäänkin hyvällä aasinsillalla kysymykseen, että olisiko Suomeen relevanttia ja ajankohtaista tuoda kotitalouksien kybervakuuttamiseen liittyviä tuotteita. Tähän B vastasi, että juuri identiteettivarkauksien varalta on jo erilaisia turvia Suomenkin markkinoilla. Sen lisäksi mahdollisuuksia varmasti koko ajan mietitään ja pohditaan, että minkälaista turvaa tähän jatkossa tarvitaan. Haastateltava C uskoi ajan olevan kypsä jo ihan silläkin verukkeella, että pohjoismaissa digitalisaatio on edennyt erittäin hyvää vauhtia ja olemme kehittyneitä koko maailman mittapuulla. Hän nosti esille myös sen, että uhka alkaa olemaan kotitalouksille jo hyvin konkreettinen, mikä on alkanut pikkuhiljaa kirkastumaan myös kotikäyttäjille. Voidaan olettaa ihmisten pitävän sitä jo todellisena riskinä, kun niin suuri osa päivittäisestä asioinnista tapahtuu verkon välityksellä.

Haastattelun lopussa ollut kysymys muista mielenkiintoisista teemoista ja ajatuksista älykotien vakuuttamiseen liittyen ei herättänyt juurikaan suuria puheenvuoroja. Kuitenkin tietoturvaa ja kyberriskejä sivuten haastateltava B mainitsi, että heidän yhtiöllänsä on tapahtumia, joissa niin sanotut ”valkoiset hakkerit” eli hakkerit, jotka eivät käytä taitojaan rikollisiin tarkoituksiin, pyrkivät yhdessä etsimään haavoittuvuuksia erilaisista järjestelmistä. Tällaisesta informaatiosta on luonnollisesti hyötyä vakuutusyhtiölle ja sitä voidaan hyödyntää myös asiakkaiden tietoturvan osalta tulevaisuudessa. Yleisesti ottaen aihetta pidettiin mielenkiintoisena ja ajankohtaisena, minkä kiteyttää hyvin C:n kommentti ”äärimmäisen mielenkiintoinen maailma ja herättää mielenkiintoa pohtia asiaa lisää”.

5 YHTEENVETO

5.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset

Tässä luvussa vastataan johdannossa esitettyihin tutkimuskysymyksiin sekä vedetään tutkielmassa käsiteltyjä teemoja yhteen johtopäätösten ja pohdintojen kautta. Tutkielmalle on asetettu kaksi erillistä tutkimuskysymystä: (1) ”Millaisena ilmiönä vakuutusyhtiöt näkevät älykoteihin kohdistuvat kyberriskit ja niiden vakuuttamisen?” ja (2) ”Mitä haasteita ja mahdollisuuksia älykotien kybervakuuttamiseen liittyy?”. Näihin kysymyksiin pyrittiin löytämään vastaukset asiantuntijahaastatteluiden avulla.

Ensimmäiseen kysymykseen saatiin melko laajalla kirjolla vastauksia ja voisi sanoa, että vakuutusyhtiöissä tunnistetaan kyberriskejä, jotka liittyvät älykotiteknologian lisääntymiseen. Yleisimpien riskien osalta esiin nousivat identiteettivarkaudet ja muut henkilötietojen väärinkäytökset. Näille riskeille altistaviksi tekijöiksi esitettiin älylaitteiden heikkoa tietosuojaa sekä käyttäjän roolia. Sen lisäksi näiden riskien vakuuttamista on selkeästi pohdittu vakuutusyhtiöissä, mistä kertoo kybervakuutuksen kaltaiset lisäturvat osana kotivakuutuksia sekä älykotivakuutuksen pilottikokeilu. Täysin yhtäläisiä näkemyksiä ei saatu kuitenkaan älykotien kyberriskien merkittävyyden ja vakuuttamispotentiaalin osalta. Yleisellä tasolla kyberriskit koetaan kasvavaksi ja jopa merkittäväksi uhaksi kotitalouksille, mutta ehkä vasta tulevaisuus näyttää kuinka vakuutusyhtiöt pystyvät reagoimaan mahdollisiin vakuutustarpeisiin.

Toisen tutkimuskysymyksen kohdalla näkökulmat myös ristesivät hieman toisistaan molempien haastattelujen osalta, mutta erilainen lähestymistapa kysymyksiin vaikutti varmasti osaltaan tähän. Merkittävimmät haasteet liittyvät vakuutettavan ilmiön epämääräisyyteen, vahinkojen akkumulaatiopotentiaaliin, tuotteen hinnoitteluun ja laitteiden standardien valvomiseen. Mahdollisuuksina sen sijaan nähtiin ennen kaikkea lisääntyvien riskien luoma tarve, älyteknologian hyödyntäminen proaktiivisessa riskienhallinnassa ja kasvava kysyntä ihmisten riskitietoisuuden lisääntyessä. Vaikka haasteita ja mahdollisuuksia osattiin jonkin verran listata, niin ilmoille jäi lopulta ehkä

lievä epävarmuus ylipäättään älykotien kybervakuuttamista kohtaan. Tähän varmasti vaikuttaa kyseisen ilmiön tuoreus sekä vakuuttamisen vaatiman datan puute.

Itse uskoisin tämän tutkielman tekemisen aikana karttuneen tiedon sekä haastattelujen perusteella, että älykotiratkaisujen yleistyminen ja siihen liittyvät riskit saattavat olla merkittäväkin uhka nyt ja etenkin tulevaisuudessa. Tämän uhkan pienentäminen sekä poistaminen on kuitenkin todella monen eri tekijän summa ja vakuuttaminen on lopulta vain yksi keino hallita älykoteihin kohdistuvia kyberriskejä. Tietoisuus riskeistä kasvaa jatkuvasti, mutta usein juuri käyttäjien rooli korostuu, kun arvioidaan riskien realisoitumisen mahdollisuutta. Toisena hyvin tärkeänä tekijänä on toki myös laitteet ja niiden heikko tietoturva, mikä tulisi ottaa aina vakavasti, kun päätöksiä älylaitteiden hankkimisesta tehdään. Tuttu sanonta ”halvalla ei saa hyvää” pätee valitettavan usein myös tietotekniikan osalta. Tästä kaikesta huolimatta odotan mielenkiinnolla millaisia suuntaviivoja tulevaisuus tuo älykoteihin liittyvien kyberriskien osalta ja kuinka vakuutusyhtiöt näihin pyrkivät vastaamaan.

5.2 Tutkielman arviointi ja jatkotutkimusehdotuksia

Tässä alaluvussa arvioidaan tutkielmaa ja lopussa esitellään mahdollisia sekä mielenkiintoisia jatkotutkimusehdotuksia aiheen tiimoilta. Tutkielman arvioinnin tarkoituksena on pohtia sekä mitata tutkielman luotettavuutta, onnistumista sekä käytettyjen menetelmien hallitsemista ja asianmukaisuutta tutkimustavoitteisiin nähden. Tässä tutkielmassa on pyritty noudattamaan mahdollisimman tarkasti hyvää tieteellistä käytäntöä kiinnittämällä erityistä huomiota muun muassa toimintatapojen rehellisyyteen ja tarkkuuteen. Näiden lisäksi on toteutettu eettisesti kestävää tiedonhankintaa ja otettu huomioon muiden tutkijoiden työ sekä annettu kunnia heidän työlleen asianmukaisella viittauskäytännöllä.

Tutkielmassa on käytetty laajasti erilaista lähdemateriaalia, joka on pääosin hyvin luotettavaa. Tutkimusmenetelmien valinta on myös perusteltu asianmukaisesti haluttuun tutkimustavoitteeseen peilaten, sillä kvalitatiivinen tutkimusmenetelmä sopii hyvin tämän kaltaiseen asetelmaan, kun pyritään aiheen syvällisempään ymmärtämiseen. Ehkä suurimpina kehityskohteina tämän tutkielman osalta voisi nostaa esille kerättyjen

aineistojen rajallisuuden ja analyysimenetelmän hyödyntämisen. Vaikka haastateltavia asiantuntijoita oli kolme ja haastatteluissa saatiin kriittistä keskustelua aikaan, niin tuloksia ei voi yleistää koskemaan molempien yhtiöiden tosiasiallista näkökulmaa, saati koko Suomen vakuutusmarkkinaa. Toisaalta tällainen yleistys ei ole edes tarkoituksenmukaista laadullisessa tutkimuksessa eikä mahdollista kandidaatintutkielman asettamien rajoitusten vuoksi. Lopulta haastatteluista saatava informaatio perustuu pitkälti haastateltavien omiin näkemyksiin ja arvioihin. Asian selvittämistä haastatteluiden avulla hankaloittaa myös se, että juuri tällaisen vakuutuksen asiantuntijoita ei oikein tahdo löytyä, koska suoranaista tuotettakaan ei ole tarjolla. Siitä huolimatta esimerkiksi yhden tai kahden lisähaastattelun avulla olisi saanut laajemman otannan sekä näin ollen luotettavampia tuloksia. Näin olisi myös voitu päästä lähemmäs aineiston saturaatiota eli kylläntymistä. Saturaatiosta voidaan puhua, kun tiedonlähteet alkavat aineiston osalta toistamaan itseään ja se on usein merkki aineiston riittävydestä. (Sarajärvi & Tuomi, 2018, 73.)

On hieman hankala verrata tutkielmaa suoraan aikaisempaan tutkimukseen, koska aiheesta on tehty erittäin niukasti tutkimusta, mutta toivottavasti keskustelu aiheen ympärillä kasvaisi ja tutkimus kehittyisi sen mukana. Yleisesti kybervakuuttamisesta ja älykodeista löytyy paljon tutkimusta, koska aiheet ovat olleet mielenkiintoisia ja ajankohtaisia jo pidemmän aikaa. Älykotien vakuuttamiseen liittyen voisi tutkia esimerkiksi kuluttajien näkemyksiä ja mielipiteitä aiheen ympärillä. Sen lisäksi olisi mielenkiintoista selvittää, millaisia rajoituksia ja hinnoittelumalleja tällaisiin vakuutuksiin tulisi sisällyttää, jotta toiminta olisi kannattavaa niin vakuuttajan kuin vakuutettavan näkökulmasta.

LÄHDELUETTELO

Kirjallisuuslähteet

- Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur*, 19(9), 139.
- Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. *IEEE transactions on systems, man, and cybernetics, part C (applications and reviews)*, 42(6), 1190–1203.
- Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, 18(3), 817.
- Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, 61, 227–232.
- Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network security*, 2016(9), 5–9.
- Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance*, 12(2), 161–185.
- Böhme, R., & Schwartz, G. (2010, June). Modeling cyber-insurance: towards a unifying framework. In *WEIS*.
- Dingli, A., & Seychell, D. (2015). The new digital natives. *Cutting the Chord. Berlin/Heidelberg*.
- Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer networks*, 44(5), 643–666.
- Eggert, M. (2019). "Understanding the acceptance of smart home-based insurances". In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019. ISBN 978-1-7336325-0-8 Research Papers.
- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*.
- Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.
- Farhan, L., Shukur, S. T., Alissa, A. E., Alrweg, M., Raza, U., & Kharel, R. (2017, December). A survey on the challenges and opportunities of the Internet of Things (IoT). In *2017 Eleventh International Conference on Sensing Technology (ICST)* (pp. 1–5). IEEE.

- Figueiredo e Silva, P., Kaseva, V., & Lohan, E. S. (2018). Wireless positioning in IoT: A look at current and future trends. *Sensors*, *18*(8), 2470.
- Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1292–1297). IEEE.
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85.
- Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537–540). IEEE.
- Harper, R. (2003). Inside the smart home: Ideas, possibilities and methods. In *Inside the smart home* (pp. 1–13). Springer, London.
- Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398–428.
- Iten, R., Wagner, J., & Zeier Röschmann, A. (2021). On the identification, evaluation and treatment of risks in smart homes: A systematic literature review. *Risks*, *9*(6), 113.
- Jiang, L., Liu, D. Y., & Yang, B. (2004, August). Smart home research. In *Proceedings of 2004 international conference on machine learning and cybernetics (IEEE Cat. No. 04EX826)* (Vol. 2, pp. 659–663). IEEE.
- Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020, April). IoT threat detection advances, challenges and future directions. In *2020 workshop on emerging technologies for security in IoT (ETSecIoT)* (pp. 22–29). IEEE.
- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671.
- Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business horizons*, *58*(4), 431–440.
- Luostarinen, K. (2021) Kyberriskit ja niiden hallintaprosessi: Case Yritys Oyj. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Kandidaatin tutkielma.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61.
- Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, *1*, 81–98.

- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sathukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, 56, 11–26.
- Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, 38(2), 226–241.
- Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *Macquarie University Faculty of Business & Economics Research Paper*.
- Pătru, I. I., Carabaş, M., Bărbulescu, M., & Gheorghe, L. (2016, September). Smart home IoT system. In *2016 15th RoEduNet Conference: Networking in Education and Research* (pp. 1–6). IEEE.
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-risk management* (pp. 33–47). Springer, Cham.
- Roikola, T. (2017). Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Pro gradu - tutkielma.
- Saad al-sumaiti, A., Ahmed, M. H., & Salama, M. M. (2014). Smart home activities: A literature review. *Electric Power Components and Systems*, 42(3–4), 294–305.
- Sarajärvi, A., & Tuomi, J. (2018). *Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos*. Tammi.
- Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, 55(4), 349–356.
- Sorri, K., Mustafee, N., & Seppänen, M. (2022). Revisiting IoT definitions: A framework towards comprehensive use. *Technological Forecasting and Social Change*, 179, 121623.
- Strupczewski, G. (2021). Defining cyber risk. *Safety science*, 135, 105143.
- Suresh, S., & Sruthi, P. V. (2015, November). A review on smart home technology. In *2015 online international conference on green engineering and technologies (IC-GET)* (pp. 1–3). IEEE.

Sähköiset lähteet

- Allianz (2022). ”The most important global business risks for 2022”, Allianz Global Corporate & Specialty, January 2022, (Viitattu: 25.10.2022), Saatavilla: <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>

- Aon (2022). "Kybervakuutus", Aon Finland, 2022, (Viitattu 24.10.2022), Saatavilla: https://www.aon.com/finland/palvelut/ratkaisut_ja_vakuutuslajit/kybervakuutus.jsp
- Basen, J. (2020). "Does Your Smart Home Need Cyber Insurance?", Residential Tech Today, 25.11.2020, (Viitattu 16.9.2022), Saatavilla: <https://restechtoday.com/does-your-smart-home-need-cyber-insurance/>
- CRO Forum (2014). "Cyber resilience – the cyber risk challenge and the role of insurance", Chief Risk Officers (CRO) Forum, December 2014, (Viitattu 25.10.2022), Saatavilla: <https://www.thecroforum.org/2014/12/19/cyber-resilience-cyber-risk-challenge-role-insurance/>
- Fennia (2022). "Tietoturvakvakuutus", (Viitattu 15.11.2022), Saatavilla: <https://www.fennia.fi/omaisuus-ja-toiminta/tietoturvakvakuutus>
- Finanssiala (2022). "Vakuutusvuosi 2021", Finanssiala, 21.4.2022, (Viitattu 15.11.2022), Saatavilla: <https://www.finanssiala.fi/julkaisut/vakuutusvuosi-2021/>
- Granato, A., & Polacek, A. (2019). "The Growth and Challenges of Cyber Insurance", Chicago Fed Letter, No. 426, 2019, (Viitattu 2.11.2022), Saatavilla: <https://www.chicagofed.org/publications/chicago-fed-letter/2019/426>
- If (2022). "Tietoturvakvakuutus", (Viitattu 15.11.2022), Saatavilla: <https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvakvakuutus>
- Kyberturvallisuuskeskus (2022). "Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt", Traficom, 12.9.2022, (Viitattu 19.9.2022), Saatavilla: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt>
- LähiTapiola (2022). "Kybervakuutus", (Viitattu 15.11.2022), Saatavilla: <https://www.lahitapiola.fi/yritys/vakuutukset/omaisuus-ja-toiminta/kybervakuutus>
- Metz, J. (2022). "Do you need personal cyber insurance for cyberattacks?", Forbes, 28.3.2022, (Viitattu 16.9.2022), Saatavilla: <https://www.forbes.com/advisor/homeowners-insurance/personal-cyber-insurance/>
- Munich Re (2022). "Munich Re Global Cyber Risk and Insurance Survey 2022", Munich Re, 2022, (Viitattu 8.11.2022), Saatavilla: <https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html>
- Pohjola Vakuutus (2022). "Kybervakuutus", (Viitattu 15.11.2022), Saatavilla: <https://www.op.fi/yritykset/vakuutukset/toiminnan-vakuutukset/kybervakuutus>

SOA (2022). "The Role of Cyber Insurance in the Smart Home Ecosystem", Society of Actuaries, 2022, (Viitattu 30.9.2022), Saatavilla:

<https://www.soa.org/research/opportunities/2022-home-ecosystem/>

Sobers, R. (2022). "166 Cybersecurity Statistics and Trends", Varonis, July 8, 2022, (Viitattu 8.11.2022), Saatavilla: <https://www.varonis.com/blog/cybersecurity-statistics#attack>

Suomen Riskienhallintayhdistys (2022). "Riskienhallintaprosessi", (Viitattu 19.11.2022), Saatavilla: <https://pk-rh.fi/riskienhallintaprosessi.html>

Turva (2022). "Kybervakuutus", (Viitattu 15.11.2022), Saatavilla: <https://www.turva.fi/yritysassiakkaat/vakuutukset/omaisuus-ja-toiminta/kybervakuutus>

Henkilölähteet

Haastateltava A, Yhtiö 1, Kehityspäällikkö ja tuoteomistaja, Yritysten omaisuus ja toiminta, Haastattelu 26.10.2022.

Haastateltava B, Yhtiö 1, Kehityspäällikkö ja tuoteomistaja, Kodin henkilö- ja omaisuusvahingot, Haastattelu 26.10.2022.

Haastateltava C, Yhtiö 2, Johtaja, Suuryritysten digitaaliset riskit ja kyberpalvelut, Haastattelu 10.11.2022.

LIITTEET

LIITE 1 Haastattelurunko

TAUSTATIEDOT HAASTATELTAVISTA

1. Kerro lyhyesti työhistoriastasi ja osaamisestasi.
2. Mikä on tämänhetkinen asemasi ja vastuut organisaatiossa, jossa työskentelet?

TEEMA 1: KYBERVAKUUTTAMINEN TÄLLÄ HETKELLÄ

3. Millaisia kybervakuutuksia yrityksenne tarjoaa ja kenelle ne on suunnattu?
4. Millaisia vahinkoja kybervakuutukset korvaavat? Entä mitkä ovat suurimpia/yleisimpiä kyberuhkia?
5. Onko kybervakuutusten ohella tarjolla muita kyberturvallisuuteen liittyviä palveluita?
6. Miten kybervakuuttaminen on muuttunut viimeisen kymmenen vuoden sisällä? Entä millaisia odotuksia on seuraavalle kymmenelle vuodelle?

TEEMA 2: KOTITALOUKSIEN KYBERRISKIT

7. Tunnistatteko erilaisia kotitalouksiin kohdistuvia kyberriskejä ja jos tunnistatte niin mitä pidätte suurimpina/yleisimpinä uhkina?
8. Onko yrityksellänne tarjolla palveluita kotitalouksiin kohdistuvien kyberriskien varalle? Jos on niin millaisia?
9. Näetkö älykotiteknologian yleistymisen olevan merkittävä kyberriski kotitalouksille nyt tai tulevaisuudessa?

TEEMA 3: ÄLYKOTIEN KYBERVAKUUTTAMINEN

10. Onko älykotien ja esineiden Internetin leviäminen tuonut uusia mahdollisuuksia kybervakuuttamiseen? Millaisia?
11. Millaisia haasteita kotitalouksille suunnatuissa kybervakuutustuotteissa voisi olla? Esimerkiksi hinnoittelun, regulaation tai haitallisen valikoitumisen suhteen?
12. Ulkomailta on jo tarjolla tämän tyyllisiä vakuutuksia, jotka suojaavat kotitalouksia kyberriskeiltä. Olisiko Suomen markkinoille relevanttia tai ajankohtaista tuoda vastaavia ratkaisuja?
13. Heräsikö haastattelun aikana muita mielenkiintoisia teemoja tai ajatuksia älykotien kybervakuuttamiseen liittyen mitä haluaisit nostaa esille?