Haaga-Helia
ammattikorkeakoulu Oy

Lähitulevaisuuden kyberuhat hotellialalla Suomessa

Maiju Nenonen
Elli Ojankoski

Opinnäytetyö
Hotellin liikkeenjohdon
koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Maiju Nenonen, Elli Ojankoski

Koulutusohjelma
Hotellin liikkeenjohto, Restonomi

Raportin/Opinnäytetyön nimi
Lähitulevaisuuden kyberuhat hotellialalla Suomessa

Sivu- ja liitesivumäärä
57 + 5

Tässä opinnäytetyössä tutkitaan mitä kyberuhkia Suomen hotelliala tulee lähitulevaisuudessa kohtaamaan. Opinnäytetyön tarkoituksena on selvittää lähitulevaisuuden kyberuhat hotellialalla Suomessa. Työn tavoitteena on hyödyttää hotellialan toimijoita näiden uhkien tunnistamisessa. Lisäksi opinnäytetyön tavoitteena on luoda informatiivinen kooste niistä lähitulevaisuuden kyberuhkista, joita hotelliala tulee kohtaamaan. Opinnäytetyö toteutettiin kvalitatiivisena tutkimuksena teemahaastatteluja käyttäen. Tutkimuksen pohjalta luotiin malli, jonka tavoitteena on auttaa hotellialan toimijoita kartoittamaan ne uhat, joita he mahdollisesti kohtaavat lähitulevaisuudessa omassa toiminnassaan. Aihe on rajattu koskemaan vain tarkoituksella aiheutettuja ulkopuolelta tulevia kyberuhkia, jotka kohdistuvat Suomen hotellialaan lähitulevaisuudessa.

Opinnäytetyön teoriaosuus koostuu kolmesta pääluvusta, jotka käsittelevät hotellialaa Suomessa, kybertoimintaympäristöä sekä kyberhyökkäysten taloudellisia vaikutuksia. Hotellialaa Suomessa tarkasteltaessa kiinnitetään huomiota teknologian kehitykseen ja megatrendeihin, jotka ohjaavat alan muutosta. Toinen tietoperustan pääluku kattaa kybertoimintaympäristön, -turvallisuuden, -uhat ja –hyökkäykset. Aiheita on käsitelty case esimerkkien kautta. Kyberhyökkäysten taloudellisia vaikutuksia käsitellään tietoperustan kolmannessa pääluvussa. Hyökkäyksistä aiheutuvat kulut ovat nousseet kansainvälisesti 23 prosenttia ja 55 prosenttia kaikista kyberturvallisuuteen laitettavista kuluista muodostuu hyökkäyksestä palautumisesta ja havaitsemisesta.

Tutkimusmenetelmänä käytettiin kvalitatiivista menetelmää. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina. Tutkimuksen tarkoituksena oli selvittää hotellialan muutosta ja sitä sen myötä lähitulevaisuudessa kohtaavat kyberuhat. Työssä tutkittiin lisäksi hyökkäyksen vaikutuksia yritykseen. Tietoperustan ja haastatteluissa syntyneiden havaintojen perusteella luotiin Kyberuhkien Kartoituksen Kidemalli. Malli auttaa hotellialan toimijoita kartoittamaan oman hotellinsa lähitulevaisuuden kyberuhkia, sen perusteella, mitkä muutokset koskevat kohdehotellia.

Tietoperustan ja haastattelujen perusteella Suomen hotellialalla kyberuhkiin ei reagoida vielä tarpeeksi. Lähitulevaisuuden suurimmat uhkia aiheuttavat muutokset hotellialalla on lisääntyvä teknologia, laaja asiakasprofiili, kyberkouluttamattomaton henkilökunta ja julkinen ilmoitusvastuu. Suurimmat näistä muutoksista aiheutuvat kyberuhat ovat luottokortti- ja henkilötietojen menettäminen, lunnasvaatimukset, maineen menettäminen, rahalliset korvaukset, kilpailuedun menettäminen, murtautuminen suljettuun lähdekoodiin ja verkkohyökkäykset.

Asiasanat
Kyberuhka, hotelliala, kyberturvallisuus, kyberhyökkäys, teknologia

Sisällys

1 Johdanto

Kybertoimintaympäristö ja erityisesti kyberturvallisuus ja –uhat ovat viime vuosina paljon esillä olleita aiheita. Kansainvälinen uutisointi herätti opinnäytetyöntekijöiden kiinnostuksen aihetta kohtaan. Eräässä uutisessa käsiteltiin itävaltalaista hotellia kohdanneita kyberhyökkäyksiä. Kyberuhkien tunnistamisen tärkeys korostuu hotellialalla suuren asiakastietomäärän vuoksi. Kyberhyökkäyksiä tapahtuu Suomen hotelliliiketoiminnassa lähes päivittäin, mutta tietoisuus kyberuhista alalla on vähäistä. Hotellialan ja kyberturvallisuuden keskinäisiä vaikutuksia ei ole Suomessa vielä juurikaan tutkittu. Opinnäytetyö haluttiin toteuttaa aiheen ajankohtaisuuden ja kiinnostavuuden vuoksi.

Pääkysymyksenä opinnäytetyössä on, millaisia kyberuhkia hotelliala Suomessa tulee kohtaamaan lähitulevaisuudessa? Pääkysymyksen tueksi laadittiin seuraavat alakysymykset. Millaisia kyberuhkia teknologian kehitys hotellialalla tuo tullessaan? Millaisia vaikutuksia kyberhyökkäyksellä on yritykseen? Mitkä kansainväliset hotellialan kyberhyökkäykset todennäköisimmin leviävät Suomeen? Mitkä toiminnot lähitulevaisuuden hotellissa ovat alttiimpia kyberuhille? Näihin kysymyksiin vastausta lähdettiin hakemaan teorian ja asiantuntijahaastattelujen kautta. Aihetta tutkittiin megatrendien, teknologian muutoksen ja kansainvälisen kybertuvallisuustilanteen avulla. Tutkimus on menetelmältään kvalitatiivinen. Tutkimuksessa haastateltiin neljää asiantuntijaa ja valinta tehtiin heidän hotellialan tai kyberturvallisuuskokemuksensa vuoksi.

Opinnäytetyön tarkoituksena on selvittää lähitulevaisuuden kyberuhat hotellialalla Suomessa. Työn tavoitteena on hyödyttää hotellialan toimijoita kyberuhkien tunnistamisessa. Lisäksi opinnäytetyön tavoitteena on luoda informatiivinen kooste niistä lähitulevaisuuden kyberuhkista, joita hotelliala tulee kohtaamaan. Tutkimus on rajattu koskemaan hotellialaa Suomessa sekä tarkoituksellisesti aiheutettuja ulkopuolelta tulevia kyberuhkia. Tutkimuksen pohjalta luodaan malli, jonka tavoitteena on auttaa hotellialan toimijoita kartoittamaan kyberuhat, joita ne mahdollisesti kohtaavat lähitulevaisuudessa omassa toiminnassaan. Työn tavoitteena on hyödyttää hotellialan toimijoita kyberuhkien tunnistamisessa.

Kyberuhkien tunnistaminen on ensiarvoisen tärkeää, sillä hyökkäysten ja uhkien määrä kasvaa vuosittain. Näiden taloudelliset vaikutukset muuttuvat koko ajan suuremmiksi, minkä vuoksi hotellialan on tunnistettava omaa toimintaansa uhkaavat kyberuhat ja niiden riskit. Kyberuhkiin varautumisessa ja niiden ennaltaehkäisyssä keskeisiä ovat kyberuhkakoulutus ja riskikartoitus.

2 Aihe ja rajaukset

Lähitulevaisuuden kyberuhat hotellialalla Suomessa valikoitui opinnäytetyön aiheeksi sen kiinnostavuuden ja ajankohtaisuuden vuoksi. Kiinnostus aiheeseen heräsi opinnäytetyön tekijöillä The New York Times lehden artikkelin ”Hackers Use New Tactic at Austrian Hotel: Locking the Doors” kautta. Artikkeli käsitteli kyberhyökkäystä itävaltalaiseen hotelliin, jossa hotellin toiminnot ajettiin alas ja niiden palauttamisesta vaadittiin lunnaita Bitcoinien muodossa. Artikkeli innoitti etsimään suomalaisia rinnakkaistapauksia, mutta kävi ilmi, ettei aihetta ole juurikaan tutkittu Suomessa, etenkään hotellialan näkökulmasta. Aihe on tärkeä, sillä kyberhyökkäyksiä tapahtuu jatkuvasti enemmän ja Suomessa hotellialan tietoisuus heitä uhkaavista kyberhyökkäyksistä on suppea. Aiheen ajankohtaisuuden ja kiinnostavuuden vuoksi opinnäytetyö haluttiin toteuttaa ja yhdistää siinä kyberturvallisuusnäkökulma hotellialaan.

Opinnäytetyössä selvitetään hotellialan näkökulmasta, mitkä ovat lähitulevaisuuden trendit ja mitä tietoturvallisuusloukkauksia maailmalla on tapahtunut. Näiden perusteella selvitetään, mitkä toiminnot ovat kriittisiä lähitulevaisuuden hotellissa Suomessa kyberturvallisuuden näkökulmasta. Opinnäytetyössä käydään läpi, miten hotelliala tulee muuttumaan ja mitä kyberuhkia sen perusteella hotelliala tulee kohtaamaan. Opinnäytetyössä myös sivutaan hotellialan nykytilaa, jotta tiedetään mistä muutos lähtee. Nykytilan arviointi on välttämätöntä muutoksen tutkimisen kannalta. Tässä opinnäytetyössä käsitellään ensin mihin hotelliala Suomessa on mahdollisesti muuttumassa pohjautuen kansainväliseen kehitykseen, jonka jälkeen kartoitetaan, millaisia kyberhyökkäyksiä hotelliala kansainvälisesti on kohdannut. Tämän lisäksi tarkastellaan kybertoimintaympäristöä, kyberturvallisuutta, -uhkia, -hyökkäyksiä sekä niiden taloudellisia vaikutuksia yritykseen. Edellä mainittujen perusteella analysoidaan, mitkä kyberuhat tulevat olemaan todennäköisimpiä hotellialalla Suomessa. Tutkimuksen perusteella luodaan malli, joka auttaa hotellialaa lähitulevaisuuden kyberuhkien kartoittamisessa ja helpottaa käytännön ennaltaehkäisytyöhön ryhtymisessä.

Aihepiiri on rajattu Suomen hotellialan tuleviin kyberuhkiin. Kyberuhkien osalta rajaus koskee tarkoituksellisesti aiheutettuja ulkopuolelta tulevia kyberuhkia. Hotelliala Suomessa on teknologisessa kehityksessään jäljessä monia muita maita. Opinnäytetyössä tarkastellaan kansainvälisiä trendejä ja hyökkäyksiä sekä haastatellaan asiantuntijoita kattavan tulevaisuuden kuvan saamiseksi. Hotellialan kyberturvallisuudesta Suomessa ei löydy juurikaan julkista tietoa, mikä on yksi peruste maantieteelliseen rajaukseen. Työssä ei myöskään kuvata kansainvälisesti tulevia kyberuhkia, sillä Suomen hotelliala on vielä perinteinen

verrattuna kansainväliseen hotellialaan. Opinnäytetyöstä rajattiin pois ehdotukset kyberuhkiin varautumiseksi ja tahattomat kyberuhat.

Opinnäytetyöllä haetaan vastausta seuraavaan pääkysymykseen:

1. Millaisia kyberuhkia hotelliala Suomessa tulee kohtaamaan lähitulevaisuudessa?

Lisäksi haetaan vastausta seuraaviin alakysymyksiin:

2. Millaisia kyberuhkia teknologian kehitys hotellialalla tuo tullessaan?
3. Millaisia vaikutuksia kyberhyökkäyksellä on yritykseen?
4. Mitkä kansainväliset hotellialan kyberhyökkäykset todennäköisimmin leviävät Suomeen?
5. Mitkä toiminnot lähitulevaisuuden hotellissa ovat alttiimpia kyberuhille?

2.1 Tutkimusmenetelmä

Tutkimusmenetelmän valinta aloitettiin pohtimalla kvantitatiivisen ja kvalitatiivisen tutkimuksen eroja ja niiden tuomia vastauksia. Ennen tutkimusmenetelmän valintaa harkittiin kvalitatiivisen ja kvantitatiivisen tutkimuksen yhdistelmää eli monistrategista tutkimusta. Tutkimukset olisi toteutettu rinnakkain, jolloin tutkittaville olisi annettu kyselylomake teemahaastattelun lopuksi. Monistrategista tutkimusta ei kuitenkaan valittu työn laajuuden vuoksi. Menetelmää valittaessa pelkällä teemahaastattelulla katsottiin saatavan tarkoituksenmukaiset ja riittävän laajat tiedot. Mikäli opinnäytetyön tutkimusmenetelmäksi olisi valittu kvantitatiivinen tutkimus, olisi siinä pyritty mittaamaan muuttujia ja lähtökohta työlle olisi ollut teoria ja hypoteesit. Tällöin tutkimusongelma olisi voinut olla seuraavanlainen ”Kuinka paljon Suomen hotellialа kohtaa kyberuhkia?”. Toisin kuin kvantitatiivinen tutkimus kvalitatiivinen tutkimus päättyy hypoteeseihin. Kvalitatiivinen tutkimussuuntaus olettaa, että muuttujat ovat toisiinsa kietoutuneita, vaikeasti mitattavia ja monimutkaisia. Koska opinnäytetyössä haluttiin selvittää, minkälaisia kyberuhkia hotelliala Suomessa tulee kohtaamaan lähitulevaisuudessa, menetelmäksi valittiin kvalitatiivinen lähestymistapa. (Hirsjärvi & Hurme 2011, 27-28, 30.)

Tutkimusmenetelmäksi valittiin haastattelu, sillä kyseessä on osittain kartoittamaton aihealue, eikä vastausten suunnasta ollut ennakkokäsitystä. Menetelmänä haastattelu antaa mahdollisuuden selventää vastauksia, syventää saatavia tietoja ja tutkia arkaluontoista aihetta haastateltavan jäädessä anonyymiksi. (Hirsjärvi & Hurme 2011, 35.) Haastateltavat esiintyvät haastatteluissa anonyymisti, sillä tutkimuksessa käsitellään arkaluontoisia yrityksiä koskevia tietoja. Anonyymiyttä perustellaan myös sillä, että haastatteluissa annetut

tiedot eivät ole julkisia. Henkilöllisyyden, yrityksen sekä aseman salaaminen mahdollisti avoimemman kysymyksiin vastaamisen. Ilman anonymiteettiä tutkimuksen tekeminen ja haastattelujen saaminen olisi ollut haastavaa, sillä yritykset eivät halua julkisesti kertoa tietoturvastaan ja yrityksiin kohdistuneista kyberhyökkäyksistä. Tämä perustuu Suomen lainsäädännössä noudatettavaan Euroopan komission asetukseen (EU) N:o 611/2013, joka ei velvoita yrityksiä julkisesti kertomaan yritykseen kohdistuneista kyberhyökkäyksistä. (Eur-Lex 2013.)

Opinnäytetyössä ei selvitetä minkään ilmiön laajuutta tai voimakkuutta, minkä vuoksi erilaiset kvantitatiiviset standardoidut mittarit, kuten kyselylomakkeet, ovat pois suljettuja. Tutkimus päätettiin toteuttaa käyttäen puolistrukturoitua haastattelumenetelmää, jota kutsutaan myös teemahaastatteluksi. Menetelmälle ominaista on, että haastattelussa jokin näkökohta on määritelty etukäteen, muttei koskaan kaikkia. Puolistrukturoidun teemahaastattelusta tekee se, että haastattelun yksi aspekti eli haastattelun aihepiirit ovat kaikille samat. Yleensä puolistrukturoiduissa haastatteluissa kysymykset ovat samat, teemahaastattelussa näin ei kuitenkaan ole, mikä sijoittaa sen lähemmäksi strukturoimatonta kuin strukturoitua haastattelua. (Hirsjärvi & Hurme 2011, 27, 35, 48.)

Tutkimusmenetelmää, -tapaa ja -aihetta valittaessa otettiin huomioon menestyksellisen ja epäonnistuneet tutkimuksen piirteitä, jotka on esitetty kuvassa 1. Opinnäytetyössä on pyritty täyttämään menestyksellisen tutkimukset piirteet. Tutkimuksen teossa on hyödynnetty opinnäytetyöntekijöiden omia hotelli- ja turvallisuusalan tai aihepiiriin muuten liittyviä kontakteja. Konvergenssi näkyy tutkimuksessa kahden eri aihealueen yhdistymisenä, sillä opinnäytetyössä yhdistyy hotelliala sekä kyberturvallisuus. Työ on erittäin ajankohtainen ja sillä pyritään luomaan hyödyllisiä, tärkeitä ja innovatiivisia vastauksia hotellialalle.

Tutkimuksen aihe oli opinnäytetyön tekijöille kybertuvallisuuden osalta tuntematon. Aihe valittiin ajankohtaisuuden ja kiinnostavuuden vuoksi eikä helppouden, nopeuden tai mukavuuden takia. Työn motivaationa ei myöskään ollut rahallinen hyöty, vaan hyödyllisen opinnäytetyön tekeminen. Siksi tutkimuksen suunnittelussa tutkimuksen kohdetta ei voitu lähestyä menetelmä edellä, vaan menetelmä piti valita tavoitteesta ja olemassa olevasta tilanteesta käsin. Aihepiiriä käsittelevät teoriat tukivat työn etenemistä. Nämä seikat tiedostamalla opinnäytetyössä on haluttu välttää epäonnistuneen tutkimuksen piirteiden toteutuminen, joihin ennen tutkimattoman aiheen käsittely joskus voi johtaa.

Kuva 1. Vertailu menestyksellisen ja epäonnistuneen tutkimuksen piirteistä. (Hirsjärvi & Hurme 2011, 13-14.)

2.2 Aineisto ja sisältö

Opinnäytetyössä käytetään lähteenä kyberturvallisuuteen ja hotellialaan liittyvää kirjallisuutta ja tieteellisiä artikkeleja. Aineistoa on kerätty myös verkossa julkaistuista artikkeleista, sillä kyberturvallisuutta hotellialan näkökulmasta on käsitelty verrattain vähän kirjallisuudessa. Case-esimerkeissä aineisto on kerätty pääsääntöisesti verkossa julkaistuista artikkeleista ja case-esimerkeissä olevien yritysten omilta verkkosivuilta. Edellä mainittujen lisäksi lähteenä on käytetty trendi- ja kyberrikosraportteja vuosilta 2017 ja 2018.

Opinnäytetyössä käytetään paljon kansainvälisiä lähteitä, koska kyberturvallisuus hotellialan näkökulmasta on käsitelty suppeasti suomenkielisissä lähteissä. Verkkojulkaistuun materiaaliin on suhtauduttu kriittisesti ja aineiston todenperäisyys on pyritty tarkistamaan useammasta lähteestä. Aineistoa on pyritty keräämään relevanteista lähteistä, kuten tunnetuista sanomalehdistä sekä arvostettujen yritysten verkkojulkaisuista.

2.3 Opinnäytetyön rakenne suhteessa tutkimusmenetelmään

Opinnäytetyö koostuu kahdesta osasta, jotka ovat tietoperusta ja tutkimus. Opinnäytetyön rakenne on esitetty kuviossa 1. Opinnäytetyön ensimmäisessä osassa käsitellään aihetta sekä tietoperustaa lähteiden kautta. Ensimmäisessä osassa on kolme osiota, jotka ovat

johdanto ja aihe & rahaukset, hotelliala Suomessa sekä kybertoimintaympäristö. Toisessa osassa tarkastellaan tutkimus, sen tulokset ja johtopäätökset. Toinen osa koostuu myös kolmesta osiosta, jotka ovat tutkimus, yhteenveto ja malli kyberuhista sekä pohdinta.

Kuvio 1. Opinnäytetyön rakenne (Nenonen & Ojankoski 2018.)

Opinnäytetyön toisessa luvussa kerrotaan tutkimusmenetelmästä ja perustellaan sen valinta. Toisessa luvussa käydään myös läpi opinnäytetyön keskeinen termistö, joka on luotu helpottamaan sen lukua. Termejä käsitellään useamman kerran opinnäytetyössä ja niiden avaaminen etukäteen tekee lukemisesta jouhevampaa.

Luvussa kolme käsitellään hotellialaa ja sen tulevaisuutta Suomessa ja käydään läpi hotellialan kyberturvallisuuden nykytilaa. Neljännessä luvussa käsitellään kybertoimintaympäristöä yleisesti, joka pitää sisällään kyberturvallisuuden, -uhat ja

-hyökkäykset. Aihetta käsitellään myös hotellien näkökulmasta ja samalla esitellään siihen liittyviä case-tapauksia maailmalta. Viidennessä luvussa esitellään kyberhyökkäysten taloudellisia vaikutuksia. Aihetta käsitellään teorian sekä case-esimerkin avulla. Esimerkissä esitellään tapaus hotellialalta sekä kerrotaan kuinka mittavia taloudellisia vaikutuksia hyökkäyksellä olisi ollut, jos se olisi tapahtunut vuonna 2018.

Kuudennessa luvussa tutkitaan lähitulevaisuuden kyberuhkia hotellialalla Suomessa teemahaastattelujen kautta. Luvussa käsitellään kyberturvallisuuden nykytilaa, hotellialan muutosta sekä lähitulevaisuuden kyberuhkia. Ennen haastattelujen läpikäyntiä esitellään haastatteluihin valitut asiantuntijat sekä kerrotaan, kuinka haastattelut toteutettiin. Seitsemännessä luvussa tehdään yhteenveto ja johtopäätökset sekä esitellään niiden pohjalta luotu malli lähitulevaisuuden kyberuhista. Viimeisessä luvussa on pohdinta ja jatkotutkimusaiheet.

2.4 Opinnäytetyön tavoitteet

Opinnäytetyön tarkoituksena on selvittää lähitulevaisuuden kyberuhat hotellialalla Suomessa. Työn tavoitteena on hyödyttää hotellialan toimijoita kyberuhkien tunnistamisessa. Lisäksi opinnäytetyön tavoitteena on luoda informatiivinen kooste niistä lähitulevaisuuden kyberuhkista, joita hotelliala tulee kohtaamaan. Tutkimuksen pohjalta rakennetaan malli, jonka tarkoituksena on auttaa hotellialan toimijoita kartoittamaan kyberuhat, joita ne omassa toiminnassaan lähitulevaisuudessa mahdollisesti kohtaavat. Malli pyrkii rajaamaan pois ne uhat, jotka eivät koske omaa hotellitoimintaa. Mallia on tarkoitus hyödyntää ennen uhka-analyysin tai muiden vastatoimien aloittamista. Opinnäytetyön tavoitteena ei kuitenkaan ole neuvoa, miten tällaisilta uhilta vältytään tai opastaa uhka-analyysin teossa.

2.5 Opinnäytetyössä käytettävä termistö

Bottiverkko on usean botin, eli tietokoneohjelman, liitos. Bottiverkko muodostuu toisiinsa kytköksissä olevista tietokoneista, jotka toistavat niille määrättyjä käskyjä. Bottiverkko on aina tavoitteellinen ja se voi olla hyvän- tai pahantahtoinen. Pahantahtoisten bottiverkkojen tavoitteena voi olla esimerkiksi roskapostitus tai palvelunestohyökkäykseen osallistuminen. (Norton; Peltomäki & Norppa 2015, 168.)

Digitalisaatio tarkoittaa asioiden ja tiedon siirtymistä fyysisestä maailmasta digitaaliseen, eli bittien maailmaan. Esimerkiksi dvd-elokuvat ovat siirtyneet nettivuokraamoihin ja suoratoistopalveluihin. (Limnell ym. 2014, 235.)

Haittaohjelma on yleistermi, jolla kuvataan tietokoneohjelmaa, joka tarkoituksellisesti aiheuttaa ongelmia tietokoneelle tai sen ympäristöön. Haittaohjelmia ovat muun muassa botit, virukset, madot ja troijalaiset. Edellä mainittujen lisäksi on olemassa myös useiden haittaohjelmien yhdistelmiä. Haittaohjelmat ovat tyypeiltään toisistaan poikkeavia ja ne toimivat eri tavoitteilla. (If 2018; Limnell ym. 2014, 236.)

Hakkeri on yleistermi henkilöstä, joka on kyvykäs murtautumaan tietojärjestelmiin. (Peltomäki & Norppa 2015, 169.) Hakkerointia on kolmenlaista, jossa eettisen hakkeroinnin tavoite on testata tietoturvaa eri kohteissa ja raportoida puutteista sekä auttaa niiden korjaamisessa. Vahingollisessa hakkeroinnissa tarkoituksena on hävittää, vakoilla tai kopioida tietoa sekä hakkeroinnin kohteen käyttämistä välikappaleena palvelunestohyökkäyksissä tai laittomien sisältöjen jakamisessa. Vahingollisten ja eettisten hakkerien välimaastosta löytyy niin kutsutut Grey Hat Hackersit, jotka saattavat käyttää kyseenalaisia tai laittomia keinoja löytääkseen tietoturva-aukkoja tai vaihtoehtoisesti hyväksikäyttää niitä. (Limnell ym. 2014, 236.)

Krakkerista käytetään yleisesti virheellisesti termiä hakkeri. Krakkeri on kuitenkin henkilö, joka murtaa kopiosuojauksia tietokoneohjelmista ja murtautuu tietojärjestelmiin aina ilman lupaa. (Peltomäki & Norppa 2015, 169.) Selvyyden vuoksi opinnäytetyössä käytetään vain termiä hakkeri, sillä näin on myös useimmissa lähteissä tehty.

Kryptovaluutta eli digitaalinen valuutta, jonka siirtäminen käyttäjien välillä toimii ilman pankkien tai valtioiden hallintaa. Kryptovaluutat pohjautuvat lohkoketjuihin ja niille on ominaista, että niitä on olemassa vain rajattu määrä. Suosituimpia kryptovaluuttoja ovat tällä hetkellä Bitcoin, Ethereum ja Ripple (XRP). (Kryptot.net.)

Kyberhyökkäys on teko tai toiminta, jolla pyritään vahingoittamaan tai käyttämään luvattomasti tietoverkkoa, -järjestelmää tai dataa. Kyberhyökkäys voi olla esimerkiksi palvelunestohyökkäys tai haittaohjelman asentaminen. Kyberhyökkäys voidaan tehdä muunkin kuin tietoverkon kautta. (Sanastokeskus TSK ry 2018, 30.)

Kyberuhka on kybertoimintaympäristöön kohdistuva haitallinen tapahtuma, joka toteutuessaan vaarantaa siitä riippuvaiset toiminnot. Kyberuhkia ovat muun muassa kyberterrorismi, kyberrikollisuus, kybervakoilu, kyberhäiriötilanne ja kybervandalismi. (Sanastokeskus TSK ry 2018, 28.)

Kybertoimintaympäristö kattaa kaikki bittien maailmassa olevat palvelut, toiminnot sekä muut tapahtumat. Kybertoimintaympäristöön kuuluu kyberturvallisuus, -uhat ja -hyökkäykset. (Limnell ym. 2014, 240.)

Kybertuvallisuus on tila**,** jossa kybertoimintaympäristöön luotetaan ja sen toiminta on turvattu**.** Kyberturvallisuudella hallitaan ennakoivasti ja tarvittaessa siedetään kyberuhkia ja niiden vaikutuksia. (Sanastokeskus TSK ry 2018, 22.)

Lohkoketju on digitaalinen tallennelista, jossa siirrot ja toiminnot ovat tallennettu pysyvästi ja anonyymisti. Tallenteet eli lohkot tietoperustassa ovat suojattuja ja niiden sisältämiä tietoja ei pysty muuttamaan tai poistamaan. Lohkoketjuun pystyy siis vain lisäämään tietoa, mutta ei muuttamaan tai poistamaan siellä olevaa informaatiota. Lohkoketjun tiedot tallentuvat useaan eri paikkaan, joka tekee sen sisältämästä informaatiosta vaikean manipuloida sekä läpinäkyvää. Jokainen lohkoon lisätty tieto on aikaleimattu, mikä tarkoittaa sitä, että kaikki data lohkoketjussa on jäljitettävää, joka tekee siitä turvatumman. (Revfine.)

Palvelunestohyökkäys on tietoverkkohyökkäys, jolla palvelu tai tietojärjestelmä pyritään lamauttamaan kuormittamalla sitä esimerkiksi suurella määrällä palvelupyyntöjä. Mikäli palvelunestohyökkäys tapahtuu yhdestä lähteestä, on se verrattain helppo jäljittää. Tästä johtuen palvelunestohyökkäykset tehdään yleensä hajautetusti (distributed denial of service attack eli DDoS). Hajautettuun palvelunestohyökkäykseen käytetään usein bottiverkkoa, jonka hyökkääjä on ottanut haltuunsa. (Sanastokeskus TSK ry 2018, 31.)

Tietoturva on tiedon suojaamista ja sen turvallisen käytön takaamista. Näiden lisäksi se koskee myös fyysisessä muodossa olevaa tietoa. Tietoturva koskettaa sähköisen tiedon säilömisen, käsittelemisen, siirtämisen, kopioimisen sekä sen julkaisemisen, salaamisen ja siihen käsiksi pääsyn. Edellä mainittujen sähköisten tietojen suojaamisen lisäksi se koskee myös kaikkea muuta tietoa. Tietoturva tarkoittaa laajimmillaan kaiken tiedon käsittelyä asianmukaisesti. (Limnell ym. 2014, 244.)

Vakoiluohjelma eli spyware on tietokoneessa ilman sen käyttäjän lupaa toimiva ohjelma, joka välittää ja kerää tietoja. Tällaisia tietoja ovat muun muassa salasanat ja sähköpostiviestit tai muu vastaava tieto. Vakoiluohjelma asentuu tietokoneeseen itsestään muiden ohjelmien asennuksen yhteydessä. Tietokonevirukset, muut haittaohjelmat, madot ja troijalaiset saattavat asentaa vakoiluohjelmia. Luottokorttinumeroita, salasanoja tai vastaavia arkaluontoisia tietoja keräävät vakoiluohjelmat ovat vakavimpia. (If 2017.)

Yöpymisvuorokaudesta käytetään myös synonyymiä yöpyminen. Tällä termillä mitataan matkailijan matkan pituutta sekä palveluiden käyttöä majoitusliikkeissä. Yöpymisvuorokauden mukaan lasketaan vuodepaikkojen käyttöaste majoitusliikkeissä. Kaikki matkan aikana tapahtuvat yöpymiset sekä yön yli tapahtuva matkustus kuuluvat kaikki mitattavaan matkan kestoon. (Tilastokeskus 2018a.)

Älyhotelli on verrattain uusi termi ja se viittaa innovatiivisiin ja älykkäisiin ratkaisuihin turismissa. Yleisimmin termillä äly viitataan teknologisiin ratkaisuihin. Älyhotelli terminä edustaa teknologiarikkaita järjestelmiä, joita käytetään hotellissa.
(Jaremen, Jędrasiak & Rapacz 2016, 1-2.)

3 Hotelliala Suomessa

Suomeen sana hotelli tuli 1830-luvulla, kun se otettiin Helsingissä käyttöön. Sanalla haluttiin erottaa korkeatasoisemmat majoitusliikkeet tavallisista majataloista. Ensimmäinen maininta majatalosta löytyy raamatusta ja sana hotelli on syntynyt alun perin 1600-luvulla Ranskassa. Hotelleiksi määritellään majoitusliikkeet, jotka tarjoavat maksua vastaan tasokasta majoitusta. Tasokkaassa hotellissa on eri huonekategorioita ja huoneistoja. Huoneessa tai huoneistossa tulee olla suihku tai kylpyhuone. Hotellin ydintuote on aina majoituspalvelu, mutta nykypäivänä hotelleissa on usein lisäksi ravintola ja kokous-, sauna- sekä kuntosalitilat. Korkeatasoisissa hotelleissa on edellä mainittujen palveluiden lisäksi myös kauneushoitola- ja kampaamopalveluita. (Rautiainen & Siiskonen 2015.)

Hotellit voidaan jaotella koon, tason, sijainnin, omistusmuodon tai kohderyhmän mukaan. Koon mukaan luokitteluita on kolme, pienet-, keskikokoiset-, ja suuret hotellit. Pienet hotellit ovat alle 100 huoneisia, keskikokoiset yli 100 huoneisia ja suuret 150 huoneesta ylöspäin. Eri tasojen mukaan jaoteltuja hotelleja voivat olla muun muassa kansalliset-, kaupalliset- ja kansainväliset hotellit. Eri omistusmuotoja hotelleissa ovat esimerkiksi osuustoiminalliset- tai yksityiset hotellit. Kohderyhmän mukaan hotellit voidaan jaotella esimerkiksi liikemies-, budjetti- ja lomahotelleihin. (Rautiainen & Siiskonen 2015.)

Suomessa hotellialaa voidaan luonnehtia perinteiseksi, sillä Suomen hotelleissa ei ole juurikaan edistyksellistä teknologiaa. Tavanomaista teknologiaa käytetään lähinnä huonevarauksissa, avainhallinnassa, asiakasrekistereissä ja muissa vastaavissa perustoiminnoissa. Kun tarkastellaan Suomen hotellitarjontaa, käy ilmi, että Suomessa ei juuri ole älyhotelleja. Myöskään seuraavien vuosien hotellihankkeet eivät anna viitteitä siitä, että tällaisia oltaisiin rakentamassa. (Raeste 2018.)

Käytössä olevia teknologisia ratkaisuja Suomessa hotelleista löytyy muun muassa Sokotelin Radisson Blu hotelleista, joissa käytössä on Radisson Blu One Touch –sovellus. Sovellus auttaa hotellivierasta tutustumaan kohteeseen interaktiivisten karttojen avulla, joista löytyy lenkkeilyreitit, nähtävyydet, ostospaikat ja ravintolat. Interaktiivisten karttojen lisäksi sovelluksesta löytyy kaikki hotellin palvelut sekä muut tärkeät tiedot alueesta. Sovelluksella asiakas voi viestiä hotellin kanssa esimerkiksi huonepalveluun, palautteeseen, huonemukavuuksiin tai uloskirjautumiseen liittyvien asioiden kanssa. (Radisson Blu, 2018.) Toinen esimerkki käytössä olevasta teknologiasta on Scandic hotelliketjulla, jolla on käy-

tössä PressReader-sovellus. PressReader tuo asiakkaan käyttöön yli 5000 sanoma- ja aikakauslehteä ympäri maailmaa. Sovelluksen käyttö vaatii puhelimen, tabletin tai tietokoneen yhdistämistä Scandicin langattomaan verkkoon. (Scandic Hotels.)

3.1 Suomen hotelliala lukuina

Vuonna 2017 Suomen majoitusliikkeissä oli lähes 22 miljoonaa yöpymisvuorokautta. Näistä 15,2 miljoonaa oli kotimaisia yöpymisiä ja loput reilu 6,7 miljoonaa ulkomaisia. Majoituspalveluiden kysyntä on ollut kasvussa vuodesta 2016 asti. Vuonna 2017 kysyntä kasvoi joka kuukausi. Vaikka venäläiset ovat edelleen suurin matkailijaryhmä ulkomaisista matkailijoista, silti merkittävin kasvu tuli Kiinasta, josta matkailijoiden määrä kasvoi 35,3 prosenttia. Japanilaisten yöpymiset taas lisääntyivät 11,1 prosenttia. Yhteensä kiinalaisten ja japanilaisten yöpymiset olivat noin puolet Aasian matkailijoiden kaikista yöpymisistä, joiden kasvu oli lähes 23 prosenttia. Suomessa oli vuonna 2017 1,1 miljoonaa aasialaisten yöpymistä, mikä on selkeästi eniten verrattuna muihin pohjoismaihin, joissa yöpymisiä kertyi 930 000. (Tilastokeskus 2018b.)

Majoitusliikkeiden määrä on Suomessa jatkuvasti kasvussa ja hotelliala kasvaa muita Pohjoismaita nopeammin. Suomen hotelliala on jäljessä verrattuna muihin Pohjoismaihin, vaikka sen kasvu onkin nopeinta. (Kauppalehti 2017.) Vuonna 2017 Suomessa tilastoituja majoitusliikkeitä oli yhteensä 1383 kappaletta, joista 672 oli hotelleja, 50 hostelleja ja loput leirintäalueita, lomakyliä tai majoituskoteja. Vuodepaikkoja majoitusliikkeissä oli yhteensä 170 092 kappaletta. Kapasiteetin kasvu keskittyi hotelleihin. (Tilastokeskus 2018b.)

3.2 Hotellialan tulevaisuus Suomessa

Hotelliala on ollut Suomessa tasaisessa kasvussa vuodesta 2016 asti. Vuonna 2016 yöpymisten määrä lähti kasvuun, jolloin Suomessa yöpymiset lisääntyivät 3,1 prosenttia. Vuonna 2017 kehitys jatkui edelleen nousujohteisena. Etenkin pääkaupunkiseudulle rakennetaan jatkuvasti uusia hotelleja, mutta myös Tampere ja jotkin pienemmät paikkakunnat kuten Himos, saavat uusia hotelleja lähivuosina. Matkailu- ja ravintolapalvelu Mara ry:n toimitusjohtaja Timo Lappi uskoo hotellialan hyvään tulevaisuuteen ja sen hyviin näkymiin. Timo Lappi kommentoi tilannetta vuonna 2017 Kauppalehdessä seuraavasti ” Eihän meillä muuten olisi hotellibuumia tai ylipäätään tehtäisi mitään hotelli-investointeja, jos näkymät olisivat huonot tai yritykset eivät luottaisi tulevaan.” (Viljanen 2017.)

Suomessa markkinat ovat lähteneet kasvuun, mikä houkuttelee uusia investoijia. Tästä johtuen kilpailu lisääntyy hotellialalla ja monet ulkomaiset ketjut laajentavat toimintaansa

Suomeen. Ulkomaisia ketjuja Suomessa on muun muassa norjalainen Clarion-ketju, yhdysvaltalainen Hilton-ketju sekä ruotsalainen Scandic hotelliketju. Hiljattain myös maailman suurin hotelliketju Marriott ilmoitti avaavansa ensimmäisen hotellinsa Suomessa Tampereelle vuonna 2019. Marriottin ja Clarionin vuoksi kiristynyt kilpailu ajaa myös kotimaiset ketjut vastaamaan kilpailutilanteeseen laajentamalla reviirejään. Hyvä esimerkki kotimaisista hotelliketjuista, jotka ovat kehittäneet hotelliverkostojaan on Lapland Hotels, joka on levinnyt Lapista Tampereelle, Ouluun sekä Helsinkiin. Lapland Hotelsin lisäksi Sokotelin hotellitketjut Sokos ja Radisson Blu ovat laajentaneet. (Autio 2017.) Myös Scandic hotelliketju leviää 15 uudelle paikkakunnalle, joista tuorein hotellihanke on Helsingin päärautatieaseman siipeen valmistuva uusi hotelli. (Raeste 2018.)

Kuten edellä jo mainittiin, aasialaisten matkailijoiden määrä on kasvussa ja he pysähtyvät entistä useammin Helsinkiin lentojen välissä. Aasiasta tulevan lentoliikenteen kasvu tekee pääkaupunkiseudusta houkuttelevamman. Tämän vuoksi hotellialan kasvu keskittyy voimakkaimmin pääkaupunkiseudulle. (Autio 2017.) Helsinkiin on kaavailtu nousevan toistakymmentä uutta hotellia vuoteen 2022 mennessä. Näiden hotellihankkeiden myötä Helsingin hotellihuoneiden määrä kasvaa melkein 4 000:lla hotellihuoneella. Helsingistä houkuttelevan tekee myös sen potentiaali kongressien järjestäjänä. Kaupungissa on jo runsaasti kansainvälisiä kongresseja, mutta majoituskapasiteetin riittämättömyys vaikeuttaa isojen kongressien saamista Helsinkiin. (Raeste 2018.)

Tällä hetkellä tiedossa oleva edistyksellisin uusi hotellihanke on vuonna 2020 valmistuva SSA Base hotelli. SSA Base on hotelli, jossa sijoittajat tai yritykset voivat ostaa itselleen hotellihuoneen tai useamman huoneen hotellikokonaisuudesta. SSA Base on uudenlainen hotellikonsepti, jollaista ei vielä Suomessa ole. Kun ostaa Base-huoneen, omistaa sen kokonaisuudessaan ja sitä voi käyttää joko omaan tarkoitukseen tai laittaa sen vuokralle. Hotellin sijoittajien ansaintalogiikka perustuu siihen, että jokainen sijoittaja saa tuottoa, vaikka oma huone olisikin tyhjänä. Tämän mahdollistaa se, että hotellia operoidaan kuten tavallistakin hotellia, vaikka omistusmuoto onkin uudenlainen. Parkkihallin, saunan ja edustustilojen tuotoista sijoittaja saa myös oman osansa. Hotellia voidaan kuitenkin pitää riskialttiina sijoituksena, sillä hotellitoiminnan menestyksellisyyttä on mahdoton arvioida etukäteen. Hotelli on suunniteltu valmistuvan vuonna 2020, jolloin markkinatilanne voi olla erilainen kuin vuonna 2018. Verkkosivujen perusteella vaikuttaa siltä, ettei hotelliin ole tulossa uudenlaista teknologiaa, kuten älylukkoja tai huoneissa olevia ohjauspaneeleita. (Hämäläinen 2018; SSA Base 2018.)

3.3 Hotellialan megatrendit

Megatrendi on suuri globaali muutossuuntaus, joka vaikuttaa laajasti. Megatrendien tunteminen on tärkeää, kun suunnitellaan liiketoimintaa. Megatrendit vaikuttavat suuresti tähän päivään ja tulevaisuuteen. (Hiltunen 2017, 37.) Trendit tarjoavat ohjausta yrityksille siitä mitä niiden omat sekä potentiaaliset asiakkaansa odottavat palvelulta tulevaisuudessa. Tulevat megatrendit voidaan karkeasti jaotella kahteen ryhmään. Nämä kaksi ryhmää ovat ihmisten tarpeet ja halut sekä ympäristön muutos. Ihmisten tarpeita ja haluja ohjaa tarve kehittää itseään, sosiaalinen statuksen korostaminen sekä yhteys muihin ihmisiin. Ympäristön muutokseen taas vaikuttavat suuret muutokset kulutuksessa, joka kattaa kaiken teknologian kehityksestä maailmanlaajuiseen taloustilanteeseen. (TrendWatching 2017.)

Tulevaisuuden kuluttajia ohjaavat TrendWatchingin mukaan 16 megatrendiä, jotka vaikuttavat vahvasti myös hotellialaan. Näitä on esimerkiksi ubitech eli kasvava kokonaisvaltainen teknologia, pricing pandemonium eli joustavampi ja moninaisempi rahankäyttö, youniverse eli yksilön tärkeyden korostuminen, joyning eli ihmisten tarve olla yhteydessä uusilla tavoilla sekä infolust eli kasvava informaation nälkä. Kaikki 16 megatrendiä on esitetty kuvassa 2. (TrendWatching 2017.)

Kuva 2. 16 megatrendiä (TrendWatching 2017.) Lupa kuvan käyttöön myönnetty Backman P. Global Futures Director, TrendWatching 6.11.2018. (Liite 5.)

Pieniä viitteitä näistä mainituista megatrendeistä näkyy Suomessa esimerkiksi Radisson Blu:lla käytössä olevasta One Touch-sovelluksesta, joka tarjoaa ratkaisua informaationälkään teknologian avulla. (Radisson Blu 2018.)

Skiftin raportissa Megatrends 2018 on listattuna 20 tärkeintä matkailualaa koskevaa megatrendiä, joista löytyy samoja teemoja kuin TrendWatchingin megatrendiraportista. Siinä missä TrendWatching:in megatrendiraporttia voidaan soveltaa lähes kaikille aloille, on Skiftin raportti keskittynyt megatrendeihin vain matkailualan näkökulmasta. Hotellialalla nämä megatrendit tulevat näkymään esimerkiksi älylaitteiden merkityksen kasvulla ongelmanratkaisijoina sekä esimerkiksi Googlen tarjoamalla saumattomalla ja kokonaisvaltaisella palveluntarjonnalla, joita ovat Google Hotels, Flights, Maps ja Trips. Tulevaisuudessa on epätodennäköistä, että erilaiset kryptovaluutat (Bitcoin, Ethereum, Bitcoin Cash ynnä muut) korvaavat tavallisen rahan kokonaan, mutta niiden käyttö lisääntyy mitä todennäköisemmin. Milleniaalit muovaavat edelleen matkailualaa ja muun muassa Etelä-Afrikassa heidän vaikutus näkyy hotellien palvelutarjonnassa nopeana langattomana verkkona sekä sosiaaliseen mediaan kelpaavina kuvattavina kohteina. Tällaisten palveluiden tarjoaminen vastaa muun muassa megatrendeihin ubitech ja status seekers. (Skift 2018, 33,53,57,62; TrendWatching 2017.)

3.3.1 Esimerkki citizenM

CitizenM hotelliketju toimii esimerkkinä osaan yllä mainituista megatrendeistä, sillä ketjun hotellit tarjoavat ratkaisua esimerkiksi youniverse, joyning ja ubitech megatrendeihin. CitizenM hotelliketjun ideologiana oli tuoda luksus kaikkien saataville ja he tekevät sen vastaamalla ajankohtaisiin trendeihin. CitizenM hotellit ovat erilaisia verrattuna perinteisiin hotelleihin. Hotelleissa on ollut alusta asti itsepalvelu sisäänkirjautuminen ilman vastaanottotiskiä, olohuoneet sekä vuorokauden ympäri avoinna oleva keittiö, jonne asiakkaat voivat kokoontua viettämään aikaa yhdessä. (citizenM.)

Megatrendit youniverse ja ubitech näkyvät citizenM konseptissa, sillä hotellihuoneen keskiössä on asiakas ja juuri hänen henkilökohtaiset tarpeensa. Tarpeisiin vastataan Moodpad-nimisellä huoneessa olevalla tablettietokoneella. Moodpadilla asiakas pystyy säätämään huoneen valaistusta, lämpötilaa, ilmastointia sekä kaihtimia omien mieltymystensä mukaan. Huoneen kokonaistunnelman voi muokata romanttisesta työskentelyyn sopivaksi. Näiden ominaisuuksien tarkoituksena on luoda uniikki ja henkilökohtainen asiakaspalvelukokemus. (Hospitality & Catering News 2012.)

3.4 Teknologian kehitys hotellialalla

Teknologia kehittyy jatkuvasti ja uusia edistyksellisiä ratkaisuja otetaan käyttöön hotellialalla. Lohkoketjuteknologia on uudenlainen tapa käsitellä informaatiota ja maksuliikennettä. Lohkoketjut ovat vieraanvaraisuusalalla vielä vähän hyödynnetty teknologia, mutta

sillä on potentiaalia kasvaa. (Revfine) Teknologian merkityksen kasvaessa, matkailijat odottavat hotelliltaan enemmän. Käytännöllisyys, saavutettavuus ja design ovat asioita, joita kuluttajat vaativat jatkuvasti kasvavassa määrin. Kuluttajien tarpeisiin voidaan vastata innovaatioiden ja teknologian avulla, kuten aiemmin mainituista megatrendeistäkin voidaan päätellä. (Kaur 2017.)

Kuten kappaleessa luvussa 3 todettiin, Suomessa hotelliala on vielä melko perinteinen. Kuitenkin uusia teknologisia ratkaisuja on alkanut saapua Suomeen. Tästä esimerkkinä toimii Hiisi Homes & Hotelsin Helsinki Haaga-hotelli, joka on ottanut käyttöön mobiiliavaimella toimivat älylukot. Älylukot valmistaa ruotsalainen Hoist Group AB Oy yritys. Lukot toimivat mobiilisovelluksen ja Bluetoothin avulla. Suojattu avain saadaan käyttöön mobiili-ilmoituksella ja sovelluksella. Tämä mahdollistaa avaimen saamisen käyttöön jo ennen hotellille saapumista ja ilman jonotusta. (Hiisi Homes & Hotels 2018; Le Gall 2017.)

Kasvaviin asiakkaiden tarpeisin vastataan kehittelemällä esimerkiksi ääniohjattua tilausjärjestelmää, tekotodellisuutta sekä biometristä tunnistusta. Biometrisellä tunnistuksella pyritään muokkaamaan prosesseista entistä saumattomampia, mikä mahdollistaa maksujen ja hankintojen tekemisen ilman lompakkoa tai puhelinta. Esimerkiksi MasterCard pyrkii saamaan markkinoille Aasiassa biometrisen tunnistuksen maksuihin ja käteisnostoihin. Tämä toimisi sormenjäljellä tai kasvojen tunnistuksella. Bulgariassa ja Etelä-Afrikassa sormenjäljellä toimivat maksukortit ovat jo käytössä. Biometrinen tunnistus perustuu kasvojen, äänen tai sormenjälkien tunnistukseen. Käytännössä tämä tarkoittaa sitä, että asiakas voi luottaa ravintolalaskun automaattiseen maksuun ilman erillistä maksutapahtumaa. Biometrisen tunnistuksen haittapuolena, sen edistyksellisyydestä huolimatta, voi olla kuitenkin lisääntynyt pelko yksityisyyden ja turvan menettämisestä. (DigFin 2018; Kobres 2018.)

3.4.1 Esimerkki Henn Na Hotel

Tokiossa sijaitseva Henn Na Hotel hyödyntää paljon robotiikkaa sekä biometristä tunnistusta ja on hotellialan edelläkävijä teknologian käytössä. Hotellin nimessäkin oleva Henn-sana tarkoittaa japaniksi muuttua, mikä edustaakin hotellin edelläkävijyyttä. Hotellissa työskentelee robotteja muun muassa vastaanotossa asiakaspalvelijoina sekä jokaisessa huoneessa henkilökohtaisena assistenttina. Nämä robotit pystyvät käymään jopa lyhyitä keskusteluja sekä antamaan illallisvinkkejä. Robotit puhuvat usealla eri kielellä ja ovat ohjelmoitu toimimaan asiakaspalvelussa myös humoristisesti.
(Henn Na Hotel; Kaur 2017.)

Biometristä tunnistusta hotellissa hyödynnetään kasvojentunnistuksella sekä esimerkiksi lämpötilan säätelyssä. Asiakkaan kirjatuessa sisään hänen kasvonsa rekisteröidään hotellin järjestelmään, jonka jälkeen ne toimivat muun muassa avaimena hotellihuoneeseen. Huoneessa ollessaan huonelämpötila säätyy automaattisesti asiakkaan ruumiinlämmön mukaan. Henn Na Hotel vastaa nykyasiakkaiden tarpeisiin sen ollessa käytännöllinen, moderni ja tarjoamalla korkeatasoista teknologiaa. (Henn Na Hotel; Kaur 2017.)

3.4.2 Lohkoketjut hotellialalla

Hotellit yhdessä muiden vieraanvaraisuusalan yritysten kanssa pystyvät lohkoketjujen avulla parantamaan palveluaan, asiakastyytyväisyyttään ja tuottavuuttaan. Mitä enemmän vieraanvaraisuusalan yritykset ottavat lohkoketjuteknologiaa käyttöönsä, sitä enemmän myös sidosryhmät alalla hyötyvät. Lohkoketjuteknologia on verkossa toimiva alusta, joka tallentaa kronologisesti käskyt ja komennot sekä jäljittää varoja hajautettujen tilikirjojen kautta. Verkossa toimivia komentoja voivat olla esimerkiksi rahasiirrot, maksut tuotteista ja palveluista, hotelli- ja lentovaraukset ja paljon muuta. Lohkoketjut yhdistetään useimmiten kryptovaluuttoihin, joilla on kaikille avoin lähdekoodi. Yritysten lohkoketjut voivat kuitenkin olla yksityisiä ja vaatia luvan käyttää niitä. (Dogru, Mody & Leonardi 2018, 1-2, 6-8.)

Lohkoketjuteknologiaa hotellialalla pystytään käyttämään muun muassa vieraiden jäljitettävyyteen, lentokenttien ja hotellien kanta-asiakas pisteisiin, digitaaliseen tunnistukseen sekä matkatoimistojen ja hotellien välisen huonemyynnin optimointiin. Lohkoketjuteknologian yksi tärkeimmistä ominaisuuksista on turvallisuus, sillä tieto jaetaan moneen eri lähteeseen. Tiedot ketjuissa on äärimmäisen hankalia hakkeroida ja hakkerointi on mahdollista vain, mikäli kaikkiin tietoa sisältäviin lähteisiin hyökättäisiin samanaikaisesti. Tietojen muuttaminen tai poistaminen ei ole mahdollista, sillä lohkoketjuun voidaan vain lisätä tietoa. Lohkoketjujen käyttöönotto mahdollisesti eliminoi väärinkäytökset ja virheet, lisäisi tehokkuutta ja turvallisuutta, vähentäisi paperityön aiheuttamia kuluja sekä parantaisi ekologisempaa inventaarion hallintaa. (Dogru ym. 2018, 2-5.)

Dogrnyn, Modyn ja Leonardin mukaan lohkoketjuteknologia eliminoisi mahdolliset väärinkäytökset ja virheet, tekien siitä turvallisemman. Kuitenkaan kaikki eivät usko lohkoketjujen turvallisuuden olevan aukotonta. Lohkoketju toimii joko avoimella tai suljetulla lähdekoodilla, jos hyökkääjä pääsee sisään suljettuun lähdekoodiin, onnistuu siirrot ilman välittäjää. Siirrot joissa kyseessä on varat, identiteetti tai informaatio ovat alttiita riskeille. Vaikka hajautettu tieto ja lohkoketjut estävät datan muutoksen jälkikäteen tai sen poistamisen, se ei kuitenkaan suojaa tietoja varkauksilta. Huonosti toimiva lohkoketjuteknologia

voi myös johtaa negatiiviseen asiakaskokemukseen. Tämä perustuu siihen, että lohkoketjujen perusrakenteen saumaton sopiminen yhteen hotellin järjestelmärakenteiden kanssa ei välttämättä toimi. (Biswas & Santhana 2017, 5-6; Dogru ym. 2018, 2-5.)

3.5 Hotellien kyberturvallisuuden nykytila Suomessa

Hotellien kyberturvallisuudesta Suomessa ei juurikaan ole julkista tietoa. Tämä perustuu Suomen lainsäädännön komission asetukseen (EU) N:o 611/2013, joka ei velvoita yrityksiä julkisesti kertomaan yritykseen kohdistuneista kyberhyökkäyksistä. (Eur-Lex 2013.) Yksi esimerkki hotellialaan liittyen on kuitenkin Hotels.com:iin liittyneet luottokorttivarkaudet. Varkaudet koskettivat satoja suomalaisia. (Vainio 2016a.)

3.5.1 Case Hotels.com

Yksi tunnetuin hotellialaan kohdistunut kyberhyökkäys Suomessa on Hotels.com hotellivaraussivustoon liitetty tietomurto. Hotels.com hotellivaraussivustosta tehtyjä rikosilmoituksia Suomessa, liittyen luottokorttien väärinkäyttöihin, oli vuoteen 2016 mennessä tehty jo 643 kappaletta. Yhteistä melkein kaikille rikosilmoituksille on ollut luottokorteilta hävinnyt raha ja maksukortin käyttäminen Hotels.com sivustolla. Vuonna 2015 Hotels.com oli mainittu rikosilmoituksissa vain 179 kertaa, joten vuoteen 2016 mennessä nousua tapahtui 259 prosenttia. (Vainio 2016a; Vainio 2016b.)

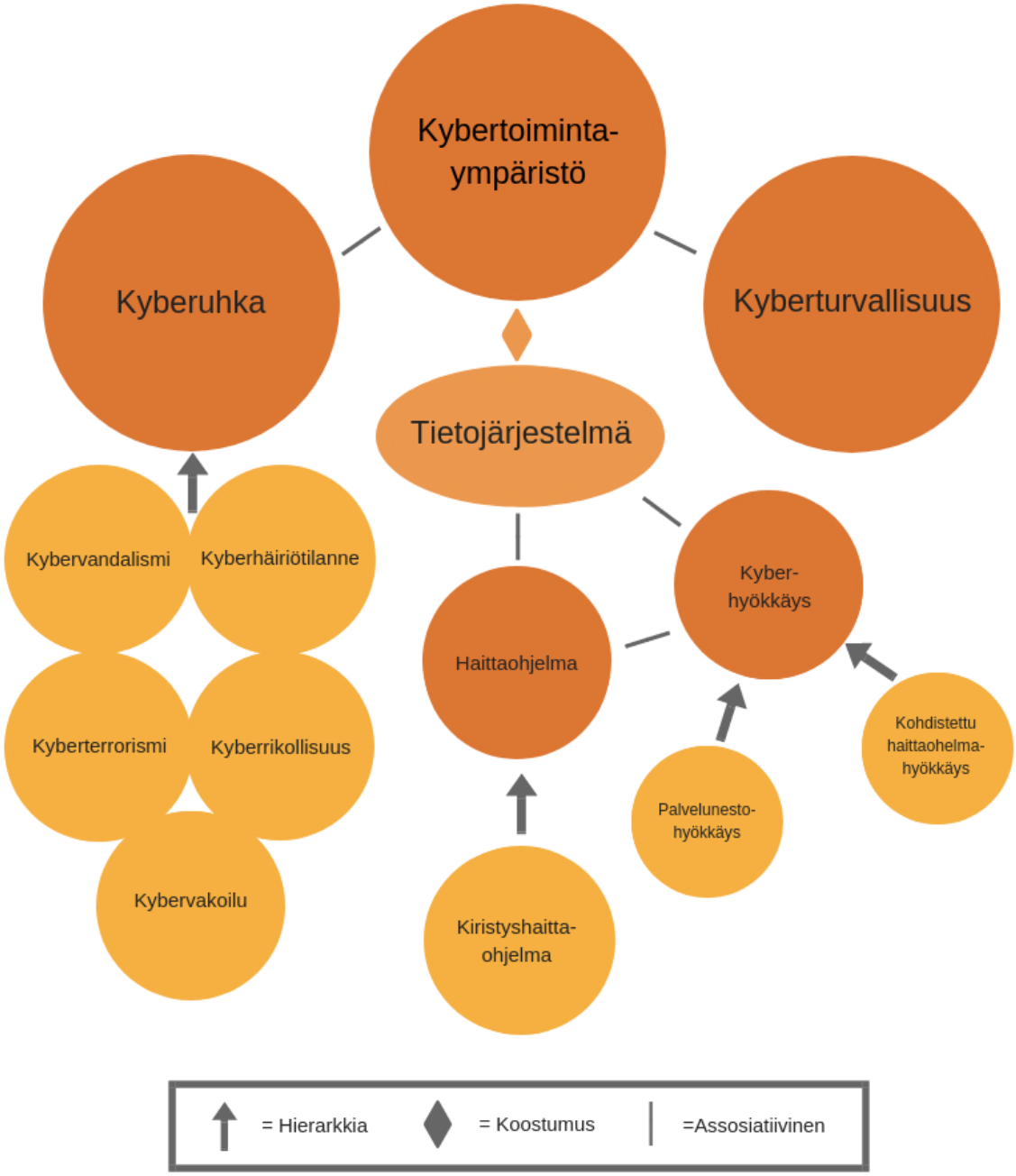
Verrattuna Hotels.com:in selkeästi suositumpaan kilpailijaan Booking.com:iin, mainitaan Hotels.com paljon useammin rikosilmoituksissa. Vuonna 2016 Booking.com mainittiin rikosilmoituksissa vain 130 kertaa. Todennäköistä siis on, että Hotels.com liittyi maksuvälinepetoksiin tai rikoksiin, jotka kohdistuivat suomalaisiin. Keskusrikospoliisin kybertorjuntakeskus teki yhteistyötä Hotels.com:in kanssa selvittääkseen mistä tietomurto johtui. Hotels.com itse kiisti, että tietovuotokohta olisi ollut heidän omissa järjestelmissään. (Vainio 2016a; Vainio 2016b.)

4 Kybertoimintaympäristö

Kreikan sana kubernetes on alun perin tarkoittanut ohjausta, kontrollia ja hallintaa. Siitä muodostunut kyber-sana on maanläheinen, vaikka kuulostaakin tekniseltä. Se tarkoittaa sellaisten järjestelmien ja niiden toimintojen turvaamista ja suojelemista, jotka ovat yhteiskunnassa arkipäivää. Kybernetiikaksi kutsuttu tieteenlaji syntyi toisen maailmansodan jälkeen. Kybernetiikka tutkii teknisten laitteiden ja elollisten olentojen keskinäistä viestintää sekä monimutkaisia säätö- ja ohjausjärjestelmiä, jotka sähkötekniikka mahdollisti. Kun internet yleistyi, alettiin kyber-alkuliitettä yhdistämään moniin termeihin, tavoittein saada niistä moderneja, esimerkiksi kyberkahvila ja kyberrikollisuus. (Järvinen 2018, 11.)

Kybertoimintaympäristö kattaa kaikki bittien maailmassa olevat palvelut, toiminnot sekä muut tapahtumat. Kybertoimintaympäristöön kuuluu kyberturvallisuus, -uhat ja -hyökkäykset. Kybertoimintaympäristö tarkoittaa siis digitaalista rinnakkaistodellisuutta. Tämä ihmisen luoma rinnakkaistodellisuus yhdistää toisiinsa ihmisiä ja laitteita valtion rajojen yli informaatioteknologian, automatisoitujen ohjausjärjestelmien, sosiaalisen median ja internetin kautta. (Limnell ym. 2014, 240.)

Kybertoimintaympäristön rakennetta on kuvattu käsitekaaviossa 1., jossa havainnollistetaan käsitteiden välisiä suhteita toisiinsa. Kaavio on luotu helpottamaan kybertoimintaympäristön kokonaisuuden hahmottamista. Käsitekaavio on yksinkertaistettu koskemaan opinnäytetyössä käsiteltäviä aiheita. Käsitesuhteita kaaviossa on kolme, assosiatiivinen suhde on kuvattu viivalla ilman symbolia, hierarkkinen suhde on kuvattuna nuolella ja koostumuksellinen vinoneliöllä. Hierarkkisessa suhteessa alakäsiteessä on kaikki yläkäsitteen piirteet, mutta se on suppeampi kuin yläkäsite. Esimerkiksi kybervakoilu on kyberuhka, mutta kaikki kyberuhat eivät ole kybervakoilua. Koostumussuhteessa alakäsite on osa yläkäsitteen kokonaisuudesta, mutta niissä ei välttämättä ole samoja piirteitä. Esimerkiksi tietojärjestelmät ovat osa kybertoimintaympäristöä, mutta kybertoimintaympäristön piirteet eivät ole samoja kuin tietojärjestelmien. Assosiatiivinen suhde tarkoittaa käsitesuhdetta, joka ei ole hierarkkinen tai koostumuksellinen. (Sanastokeskus TSK ry 2018, 9.)



Käsitekaavio 1. Kybertoimintaympäristö (Sanastokeskus TSK ry 2018, 10, 24, 28, 33.)

Tietotekniikan nopea kehittyminen ja digitaaliset globaalit verkot ovat mahdollistaneet suuria taloudellisia kasvuja ja innovaatioita yrityksille. Se myös mahdollistaa uusien yritysten luomisen sekä sosiaalista osallistumista ja demokratiakehitystä. Nopean kehityksen vuoksi teollisuus, terveydenhuolto, vesi- ja energiahuolto sekä liikenne ovat nykyään riippuvaisia kybertoimintaympäristöstä. Tämä ympäristö on kuitenkin haavoittuva ja kehityksen myötä on syntynyt uusia uhkia, kuten kyberhyökkäykset, kybervakoilu ja muuta kyberrikollisuutta. Kybertoimintaympäristön luotettavuus ja turvallisuus ovat tärkeitä, jotta ympäristön tuomia mahdollisuuksia voidaan hyödyntää oikein. (Ulkoministeriö.)

4.1 Kyberturvallisuus

Peltomäki ja Norppa (2015, 170) määrittelevät kyberturvallisuuden seuraavasti ”Kyberturvallisuus: Tietoturvaa laajempi käsite. Kyberturvallisuudella varmistetaan, että kybertoimintaympäristöön voi luottaa ja sen tarkoituksenmukaisesta toiminnasta voidaan huolehtia.”. Toisin sanoen, kyberturvallisuus kattaa ennakoivasti hallittavat ja siedettävät kyberuhat, joista ei aiheudu merkittävää haittaa yritykselle tai sen sähköisen tiedon toiminnalle tai sen toimivuudelle. Tietoturvan tavoitteena on suojata tietojärjestelmää ja sen tietoja, kun se pettää on kyberturvallisuuden toiminta uhattuna. Kyberturvallisuus on aina tietoverkossa ja sen tavoitteena on taata ihmisten ja yritysten tietojen liikkuminen turvallisesti. (Peltomäki & Norppa 2015, 67-68.)

Toisin kuin usein luullaan hakkerit harvoin luottavat ainoastaan tietoturva-aukkoihin ja omiin kykyihinsä. Isolta osin kyberhyökkääjät luottavat tavallisten ihmisten tekemiin virheisiin. Hakkerien luottaessa inhimillisiin virheisiin, kouluttaminen ja kouluttautuminen ovat järkeviä ja hyödyllisiä keinoja vähentää kyberuhkien riskiä. (Bradford 2018.)

Suurien rahasummien käyttäminen turvallisuusteknologiaan voi tuoda turvallisuuden tunteen. Missä tahansa kyberuhassa ensimmäinen ja viimeinen puolustus on johtajilla ja työntekijöillä. Valmistautuakseen ja ehkäistäkseen kyberhyökkäyksiä tulevaisuudessa, yritysten olisi hyvä tasapainottaa teknologia sekä ihmiskontakti keskenään. Työntekijöiden välinpitämättömyys tai tietämättömyys voi tulla yritykselle erittäin kalliiksi. Sen lisäksi, että työntekijän tulee tietää ja ymmärtää yrityksen käytännöt kyberturvallisuuteen liittyen, tulisi heidät myös kouluttaa tunnistamaan epäilyttävä ja pahantahtoinen toiminta. Kaikkien yrityksen hallituksesta työntekijöihin tulisi olla valppaita tunnistamaan riskejä. Omien työtekijöiden lisäksi myös eri sidosryhmien henkilöiden kouluttamisen tärkeys korostuu. Kouluttamiseen sijoittamisen tärkeyttä voidaan kuvata esimerkiksi autolla, jossa on kaikki uusimmat turvallisuusteknologiat, mutta tärkein turvallisuuselementti on silti osaava kuski. Jo pelkästään tällaisella toiminnalla pystytään säästämään suuria summia rahaa. (Disparte & Furlow 2017.)

4.1.1 Case Bangladesh Central Bank ja New York Federal Reserve Bank

Vuonna 2016 helmikuussa Bangladesh Central Bank ja New York Federal Reserve Bank joutuivat hakkerin hyökkäyksen kohteeksi. Hakkerit yrittivät siirtää noin miljardi Yhdysvaltain dollaria varastetuilla valtakirjoilla New York Federal Reserve Bankin tililtä Bangladesh Central pankista. Hakkerit olivat luoneet neljä siirtopyyntöä yhteissummalla 81 miljoonaa ja viidennen, joka oli suuruudeltaan 20 miljoonaa. Rahojen oli tarkoitus päätyä Filippiineille sekä Sri Lankaan. Välityspankkina hakkerit käyttivät Deutsche Bankia, jossa huomattiin

viidennessä siirtopyynnössä olevan kahden kirjaimen kirjoitusvirhe. Hakkereiden oli tarkoitus kirjoittaa kansalaisjärjestö NGO Shalika Foundation, mutta kirjoittivatkin NGO Shalika Fandation. Saksalainen pankkivirkailija jäädytti siirron kysyäkseen vahvistusta Bangladeshin keskuspankilta. Vastaavanlaisia siirtoja alettiin tutkia ja kaiken kaikkiaan hakkerien siirtoja onnistuttiin pysäyttämään yhteensä 850-870 miljoonan dollarin edestä, eli melkein miljardi Yhdysvaltain dollaria. (Quadir 2016.)

Hyökkäyksen suorittaneita hakkereita ei onnistuttu jäljittämään ja Bangladeshin viranomaiset kertoivat, että rahojen palauttaminen voi viedä kuukausia, mutta todennäköistä on, ettei niitä koskaan saada palautettua kokonaan. New York Federal Reserve Bank ja Bangladesh Central Bank tekivät yhteistyötä selvittääkseen, kumman järjestelmien kautta hyökkäys suoritettiin. Tutkimuksessa selvisi, että Bangladesh Central Bank:in rahasiirroista vastuussa olevan virkailijan tietokoneeseen oli hakkeroiduttu ja sitä kautta hyökkäykset olivat mahdollistuneet. (Gopalakrishnan & Mogato 2016; Quadir 2016.)

Deutsche Bankin pankkivirkailijan valppauden ja hyvän koulutuksen avulla pystyttiin estämään suurempi vahinko. Ilman pankkivirkailijan tarkkaavaisuutta olisi rahalliset menetykset nousseet melkein miljardiin Yhdysvaltain dollariin. (Quadir 2016.)

4.2 Kyberuhat

Kyberuhalla tarkoitetaan tekoa tai tapahtumaa, joka toteutuessaan vaarantaa sellaiset toiminnot, jotka ovat riippuvaisia kybertoimintaympäristöstä. (Peltomäki & Norppa 2015, 170.) Turvallisuus on käsitteenä suhteellinen ja sen taso riippuu uhasta. Uhkia voivat olla sellaiset asiat, jotka estävät tai vaikeuttavat toimintaa tai muulla tavoin aiheuttavat vahinkoa. On otettava huomioon, että suurin osa kyberuhkista, jotka toteutuvat eivät ole tarkoituksellisesti aiheutettuja. Tällaisen toimimattomuuden taustalla ovat usein ohjelmistovirheet tai tekniset viat. Paljon yleisempää on siis tahattomat häiriöt ja katkokset, kuin tarkoituksella aiheutetut. Uhka-analyysi on hyvä keino määrittämään turvattavan kohteen kyberuhkia. (Limnell ym. 2014, 37-38.)

Uhka-analyysit ovat aina ennustamista tulevasta, sillä kuten aiemmin mainittu, turvallisuus on suhteellista ja uhkan tasosta riippuvaista. Uhka-analyysilla arvioidaan millaiset uhat uhkaavat yritystä ja miten vakavasti ne voivat vahingoittaa yritystä tai yritykselle tärkeitä arvoja. Uhka-analyysin tärkeimmät kysymykset ovat, mitä turvataan, eli kuinka toimitaan, jos turvallisuus pettää sekä miltä turvataan, eli mikä uhkaa määritetyn kohteen turvallisuutta. (Limnell ym. 2014, 37-38.)

Yleisimmiksi kyberuhiksi yleisesti määritellään haittaohjelmat, verkkohyökkäykset, mobiili applikaatioihin kohdistuvat hyökkäykset, palvelunestohyökkäykset sekä bottiverkot, eli yhteen kytketyt kaapatut verkot. (ENISA 2017.) Hotellialan viisi suurinta kyberuhkaa ja –haastetta on taas luottokorttitietojen varastaminen, langattoman verkon kautta tehdyt hyökkäykset, joilla on varastettu henkilökohtaisia tietoja ja salasanoja, uhka-analyysin ja turvallisuusauditointien puute, fyysiset rikokset, joilla asetetaan hotelli vaaraan sekä kilpailuedun menettäminen, joka johtuu esimerkiksi verkossa olevan maineen heikentymisestä. (Shabani 2016, 9.)

Hotellien yleinen heikko kohta on huoneiden ovissa olevat lukitusjärjestelmät. Ympäri maailmaa käytössä olevasta Assa Abloy Vison by Vingcard järjestelmästä löytyi haavoittuvuus, jonka saivat selville suomalaiset Timo Hirvonen ja Tomi Tuominen. Hirvonen ja Tuominen loivat laitteen, jolla hotellin yleisavaimen saa luotua kopioimalla minkä tahansa avainkortin käyttäen Proxmark3 ohjelmoitavaa lukijaa. Proxmar3 on tavallinen ja sen voi tilata kuka tahansa nettikaupasta. Yleisavaimen luominen laitteelle on yksinkertaista. Ensimmäisessä vaiheessa kopioidaan kyseessä olevan kiinteistön avain ja sen jälkeen se viedään saman kiinteistön lukon lähelle, jolloin laite etsii yleisavaimen eri avainvaihtoehdoista. Kopioinnin jälkeen laite on yleisavain, joka toimii koko hotelliin ja yleisavaimen voi kopioida laitteelta mille tahansa uudelle avainkortille. Hirvonen ja Tuominen ilmoittivat Assa Abloy yhtiölle löydöksestään heti, jonka jälkeen lukkoihin tuli suorittaa suojaava päivitys. Vaikka yleisavaimen luominen ja murtautuminen lukkojärjestelmään oli helppoa, ei Tuominen kuitenkaan usko ammattirikollisten murtautuvan hotellihuoneisiin tällä tavoin. Löydetty haavoittuvuus ei kuitenkaan koske uusinta lukkojärjestelmää. Turvallisuusratkaisut eivät ole ikuisia, joten tuotekehittelyä on jatkettava, mikäli haavoittuvaisuuksilta halutaan välttyä. (Rissanen 2018.)

Hotellit pystyisivät estämään tällaisten uhkakuvien toteutumisen verrattain helposti. Kiinnittämällä huomiota esimerkiksi seuraaviin asioihin voitaisiin välttää yleisimpiä kyberhyökkäyksiä: kunnolliset palomuurit, luottokorttitietojen oikeanlainen säilytys, salasanojen päivittäminen, turvallisuuden tarkastamatta jättäminen sekä kolmansien osapuolien pääsyn valvominen hotellin tietojärjestelmiin. Edellä mainitut toimenpiteet saattavat vähentää kyberhyökkäyksiä, mutta ne eivät poista niiden uhkia kokonaan, sillä uusia tapoja hyökätä järjestelmiin syntyy koko ajan. (Shabani 2016, 9-10.)

4.3 Kyberhyökkäys

Limnell, Majewski ja Salminen (2014, 140) määrittelevät kyberhyökkäyksen seuraavasti ”Bittien maailman kautta tapahtuva hyökkäys, jolla voidaan tuottaa haittaa, vahinkoa tai

tuhoa sekä fyysiseen että bittien maailmaan. Kyberhyökkäyksen tarkoituksena voi olla myös tiedon varastaminen tai laitteiden ja järjestelmien käytön estäminen.”

Kyberhyökkäyksistä voi puhua myös kyberrikollisuutena, mikäli hyökkäys on rikos oikeustieteellisen määritelmän mukaan, eli tahallinen teko tai laiminlyönti, joka on lain mukaan rangaistava teko. Kyberrikollisuudesta käytetään myös termejä tietoverkkorikos ja tietotekniikkarikos. (Peltomäki & Norppa 2015, 34.)

Hotellit ovat yleinen ja helppo kohde hakkereille. Tähän on osasyynä verkossa ja tietokoneilla olevat toiminnot, jotka kattavat hotellien melkein jokaisen päivittäisen tehtävän. Tämän lisäksi monissa hotelleissa, niiden ollessa pieniä tai yksityisiä, ei vielä ole laajoja turvallisuusjärjestelmiä. Hotellit kohtaavat tällä hetkellä eniten kolmenlaisia hyökkäyksiä, lunnasvaatimukset, varaus- ja myyntijärjestelmien hakkerointi sekä langattoman verkon kautta tapahtuvat hyökkäykset. Lunnasvaatimushyökkäykset perustuvat datan tai muiden järjestelmien alas ajamiseen, jolloin hotellilta voidaan vaatia tietty summa lunnaita niiden palauttamiseksi. Tätä tapaa käytettiin esimerkiksi Itävallassa hotelli Seehotel Jägerwirtissä, jossa elektroniset avaimet lamautettiin ja palautettiin käyttöön hotellin maksettua lunnaat. Varaus- ja myyntijärjestelmien kautta tehdyt hyökkäykset ovat hakkerien suosiossa, niiden suuren tietomäärän vuoksi. Yksi suurimmista tämän tyyppisistä tietomurroista tapahtui HEI Hotels & Resorttien järjestelmiin. Yhtiön portfoliossa olevista hotelleista kahteenkymmeneen hyökättiin ja näiden hotellien joukossa oli muun muassa Starwood ja Marriot International. (Kevin Davis Insurance Services 2018) Toinen esimerkki tietojärjestelmien hakkeroinnista on Sabre Hospitality Solutions-järjestelmän SynXis-keskusvarausjärjestelmään asennettu haittaohjelma, joka vaaransi The Trump Hotel Collection hotellien asiakastietoja. (The Trump Hotels 2017.) Viimeisin suurimmista hyökkäyksistä on langattoman verkon kautta tapahtuva henkilökohtaisten tietojen varastaminen. Tällaisissa hyökkäyksissä asiakkaan tiedot varastetaan niin kutsutun välikäden kautta, jolloin asiakkaan puhelimeen tai muuhun mobiililaitteeseen päästään käsiksi, kun asiakas kirjautuu langattomaan verkkoon. (Kevin Davis Insurance Services 2018)

Kyberhyökkäyksiä ja -rikoksia kehitetään jatkuvasti monimutkaisemmiksi ja fiksummiksi hakkerien toimesta. Hakkerit ja rikolliset kehittävät itseään ja tapoja hyökätä niin, että rikoksien suorittaminen helpottuisi. Maailmanlaajuisesti katsottuna jo pelkästään lunnasvaatimushyökkäysten toistuvuus on noussut 13 prosentista 27 prosenttiin vuodesta 2016 vuoteen 2017. (Accenture 2017, 3-4.)

4.3.1 Case Hyatt

Hyatt hotelliketju on joutunut kyberhyökkäysten kohteeksi kahdesti. Ensimmäisen kerran hyökkäys tapahtui vuonna 2015, jolloin maksukorttitiedot varastettiin. Hyökkäys kosketti 250 hotellia 50 maassa. Toinen kyberhyökkäys tapahtui vuonna 2017, joka myös kohdistui maksukorttitietoihin. Kyseinen tietomurto oli hieman pienempi kuin vuonna 2015 tapahtunut ja kosketti vain 41 hotellia 11 eri maassa. (Ajmera 2017; KrebsonSecurity 2016.)

Vuonna 2015 elokuusta joulukuuhun välisenä aikana Hyatt:in asiakkaiden maksukorttitiedot varastettiin. Kyberhyökkäyksen kohteeksi joutui pääsääntöisesti Hyatt:in ravintoloissa käytetyt maksukortit. Pieni osa kylpylässä, parkkihallissa ja golf-kaupassa käytetyistä korteista joutuivat myös riskialttiiksi. Hyökkäys tapahtui asennetun haittaohjelman kautta, joka oli suunniteltu keräämään maksukortin tiedot, eli kortin numero, voimassaoloaika, kortinhaltian nimi sekä turvakoodi. Haittaohjelma oli suunniteltu keräämään kortin tiedot maksutapahtumien kautta eikä muita henkilökohtaisia tietoja, kuten henkilötunnuksia, vaarantunut. Hyatt hotelliketju joutui tekemään kattavan tutkinnan yhdessä kyberturvallisuusasiantuntijoiden kanssa selvittääkseen ongelman ja vahvistaakseen järjestelmien turvallisuutta. (Hyatt 2016.)

Uudempi hyökkäys tapahtui maaliskuun ja heinäkuun 2017 välisenä aikana kohdistuen jälleen kerran maksukorttitietoihin. Hyökkäys huomattiin heinäkuussa, mikä tarkoitti, että se oli ollut käynnissä jo viisi kuukautta. Laajuudeltaan uudempi hyökkäys oli pienempi kuin edellinen. Uusi hyökkäys vaati silti sisäisen tutkinnan ja toimenpiteitä, jotta tällaista tapausta ei tulisi enää vastaisuudessa. (Ajmera 2017.)

Hyatt hotelliketju on menettänyt suuren määrän asiakkaiden luottokorttitietoja omien järjestelmien kautta. Kaikissa tapauksissa luottokorttitiedot menetettiin järjestelmiin asennettujen haittaohjelmien takia.

4.3.2 Case The Trump Hotel Collection

The Trump Hotel Collection hotelleihin on viime vuosien aikana kohdistunut tietävästi ainakin kolme kyberhyökkäystä, joista uusin tapahtui elokuun 2016 ja maaliskuun 2017 välisenä aikana. Tällä aikavälillä Sabre Hospitality Solutions varausjärjestelmästä tulleiden varausten kautta asiakkailta vietiin henkilökohtaisia tietoja, kuten osoite-, luottokortti- ja puhelinnumerotietoja. Vaikka hyökkäys tapahtui Sabre Hospitality Solutions-järjestelmän kautta, eikä siten vaarantanut Trump hotellien omia järjestelmiä, ovat Trump hotellit silti joutuneet vastaavien hyökkäysten kohteeksi aiemminkin. (Bhattarai 2017.)

The Trump Hotel Collection julkaisi tiedotteen koskien 2016-2017 aikavälillä tapahtunutta kyberhyökkäystä. The Trump Hotel Collection ilmoitti, että tilanteen selvittämisessä tehtiin yhteistyötä Sabren, viranomaisten sekä luottokorttiyhtiöiden kanssa. Hyökkäykset tehtiin Sabre Hospitality Solutions-järjestelmän SynXis-keskusvarausjärjestelmän kautta. (The Trump Hotels 2017.)

Vanhin hyökkäys oli vuonna 2014 Trump hotellien maksujärjestelmiin asennettu haittaohjelma, joka kaivoi esille asiakkaiden luottokorttitietoja yli vuoden verran, kesäkuuhun 2015 asti. Toisen kerran Trump hotellien järjestelmiin hyökättiin marraskuussa 2015, jolloin haittaohjelma oli asennettu 39 järjestelmään ja sen vaikutus koski viittä hotellia. Vakoiluohjelma oli asennettu perintäjärjestelmään ja sai haltuunsa henkilökohtaisia tietoja, kuten nimen ja henkilötunnuksen yli 300 ihmiseltä sekä yli 70 000 luottokorttinumeroa. Tiedot joutuivat alttiiksi väärinkäytölle. (Bhattarai 2017.)

The Trump Hotel Collection on menettänyt suuren määrän asiakkaiden henkilö- ja luottokorttitietoja omien sekä sidosryhmien kautta. Henkilö- ja luottokorttitiedot menetettiin järjestelmiin asennettujen haittaohjelmien eli vakoiluohjelmien kautta.

4.3.3 Case Seehotel Jägerwirt

Poikkeuksellinen lunnasvaatimushyökkäys tapahtui itävaltalaisessa Seehotel Jägerwirtissä kun hakkerit murtautuivat hotellin järjestelmiin, lamauttaen ne ja lukiten vieraat ulos huoneistaan. Järjestelmien palauttamiseksi takaisin käyttökuntoon hakkerit vaativat kahden Bitcoinin lunnaita (silloinen arvo yhteensä noin 1800 Yhdysvaltain dollaria). (Bilefsky 2017.)

Seehotel Jägerwirt on joutunut samanlaisen hyökkäyksen kohteeksi jo kolmesti. Hotellin kyberturvallisuustoiminnot uusittiin ja paranneltiin viimeisimmän hyökkäyksen jälkeen ja tietokoneet sekä muut puolustusjärjestelmät korvattiin uusilla. Siitäkin huolimatta, että hotellin turvajärjestelyjä paranneltiin, hotellinjohtaja Cristoph Brandstaetter kertoi hotellin vaihtavan sähköiset lukkonsa tavallisiin. Vaikka hyökkäyksen muoto onkin poikkeuksellinen hotellien keskuudessa, eivät lunnasvaatimushyökkäykset silti ole tavattomia. Noin joka neljäskymmenes sekunti tapahtuu lunnasvaatimushyökkäys, jotka kohdistuvat pääsääntöisesti yrityksiin muilla aloilla. (Oberhaus 2017.)

Seehotel Jägervirt case osoittaa älylukkoihin ja järjestelmiin liittyviä riskejä. Toistuvat lunnasvaatimushyökkäykset ajoivat hotellin vaihtamaan lukitusjärjestelmänsä.

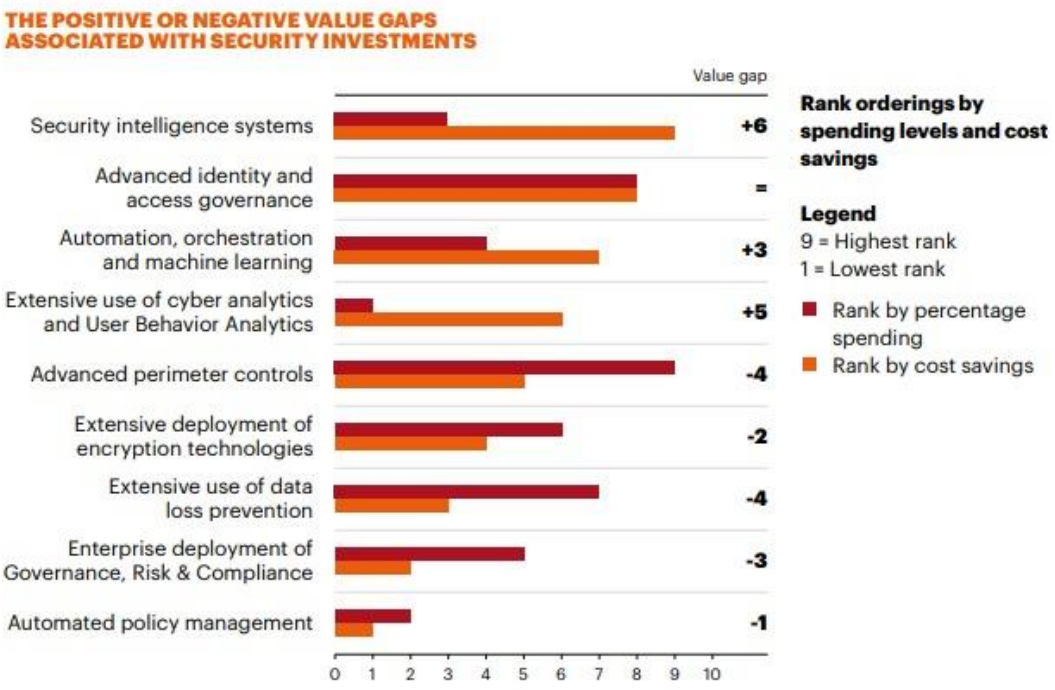
5 Kyberhyökkäysten taloudelliset vaikutukset

Kyberhyökkäyksillä ja –rikollisuudella on vaihtelevia vaikutuksia eri alojen toimijoihin. Aiheutuneet vahingot sekä menetykset eivät ole verrannaisia, vaan riippuvat ne aina toimialasta ja kilpailutilanteesta. Kyberyökkäyksen kohteeksi joutunut yritys voi kärsiä tietopääoman tai luottamuksellisen tiedon menetyksestä, hukatuista mahdollisuuksista tai vahingoittuneesta maineesta taloudellisten menetysten ohella. Lisäkustannuksia kyberhyökkäyksistä koituu yritykselle paranneltavien tietojärjestelmien ja –verkkojen myötä sekä mahdollisille asiakkaille tai yhteistyökumppaneille maksettavista korvauksista. Accenturen tutkimuksen mukaan 55 prosenttia kyberturvallisuuteen laitettavista kuluista muodostuu yrityksillä hyökkäyksestä palautumiseen ja havaitsemiseen käytetyistä varoista. Samalla kun havaitsemiseen on sijoitettu enemmän, on vastaavasti palautumiseen mennyt vähemmän rahaa. Tämän vuoksi organisaatiot, jotka systemaattisesti pystyvät palautumaan ja sen myötä parantamaan havaitsemisprosessia saavuttavat selvää rahallista etua. Kaikkia kyberhyökkäyksen aiheuttamia vahinkoja on hankala jäljittää tai muuttaa rahaksi, josta johtuen kyberhyökkäyksen kokonaisvaltaista taloudellista menetystä on hankala määrittää. (Accenture 2017, 30; Limnell ym. 2014, 126-127.)

Accenturen tuoreimman tutkimuksen mukaan kyberhyökkäyksestä aiheutuvat kulut ovat nousseet vuoden aikana jopa 23 prosenttia kansainvälisesti. Tilanne vieraanvaraisuusalalla ei kuitenkaan kulujen osalta ole huono verrattuna rahoitusalaan. Rahoitusalalla kyberhyökkäyksistä aiheutuvat kulut vuodessa yltävät 18,28 miljoonaan, kun taas vieraanvaraisuusalan kulut ovat 5,04 miljoonaa. Tutkimuksessa tutkittiin myös, millaisilla kyberhyökkäyksillä on suurimmat taloudelliset vaikutukset yrityksiin. Kaikista haitallisin kyberhyökkäys yritykselle taloudellisesti on tutkimuksen mukaan haittaohjelmat, toiseksi haitallisin verkossa tapahtuvat hyökkäykset ja kolmanneksi palvelunestohyökkäykset. Kaiken kaikkiaan yritykset käyttävät keskimäärin 2.4 miljoonaa Yhdysvaltain dollaria haittaohjelmien aiheuttamien ongelmien korjaukseen. Bottiverkot ja lunnasvaatimukset ovat yksittäiskustannuksiltaan yritykselle vähiten haitallisia taloudellisesti, mutta ne ovat taas vastaavasti toistuvampia kuin haittaohjelmat. (Accenture 2017, 20, 27.)

Datan ja informaation menettäminen hyökkäyksessä edustaa yhtä suurimmista yksittäisistä kuluista kyberhyökkäyksissä. Tämän kaltaiset hyökkäykset ovat toistuvuudellaan nousseet 35 prosentista 43 prosenttiin vuosien 2015 ja 2017 välisenä aikana. Tämän kaltaisten uhkakuvien vuoksi yritysten tulisi miettiä uudelleen rahallisia sijoituksiaan suojausteknologiaa ajatellen. Tällä hetkellä monet organisaatiot kansainvälisesti käyttävät liian

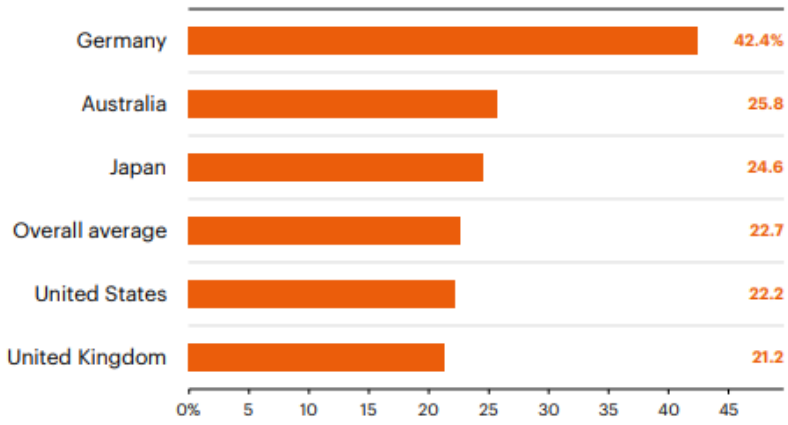
paljon rahaa vääriin osa-alueisiin. Kuviosta 2. selviää, että viidessä yhdeksästä teknologian osa-alueesta oli negatiivinen arvo, kun verrataan käytettyä rahaa ja kustannussäästöjä. Jäljelle jäävistä neljästä osa-alueesta kolmella on selkeä positiivinen arvo ja yksi on tasapainossa. Kuvio 2. auttaa arvioimaan sellaisia osa-alueita, joilla rahaa käytetään liikaa sekä tasapainottamaan se niiden osa-alueiden kanssa, joihin rahaa ei sijoiteta tarpeeksi. (Accenture 2017, 4-5.)



Kuvio 2. Positiivinen tai negatiivinen kuluero suhteutettuna turvallisuusinvestointeihin. (Accenture 2017, 5.)

5.1.1 Kyberturvallisuuden taloudellinen muutos vuosina 2016-2017

Kyberrikollisuudesta johtuvat kulut ovat kasvaneet merkittävästi vuosien 2016 ja 2017 välisenä aikana. Merkittävin kasvu on tapahtunut Saksassa, jossa kulut ovat nousseet jopa yli 40 prosenttia. Kulut ovat nousseet keskiarvoisesti noin 20 prosenttia, myös muissa maissa on tapahtunut huomattavaa kulujen kasvua kuten kuviosta 3. näkyy.



Kuvio. 3. Prosentuaalinen nousu kyberturvallisuuden kuluissa 2016-2017. (Accenture 2017, 14.)

5.1.2 Case Hilton Worldwide Holdings Inc

Vuonna 2014 loppuvuodesta ja vuoden 2015 kevään ja kesän aikana Hilton Worldwide Holdings Inc joutui tietomurron kohteeksi. Tietomurto altisti 363 000 luottokortin tiedot väärinkäytölle. Hiltonin brändeihin kuuluut mm. Waldorf Astoria, Homewood Suites, Embassy Suites, Conrad ja DoubleTree, jotka altistuivat hyökkäykselle. Hilton joutui maksamaan 700 000 Yhdysvaltain dollarin korvaukset, sillä heillä oli huomattavia puutteita datan suojaamisessa ja he epäonnistuivat kommunikoimaan tietomurroista asiakkaille ajoissa. Korvausten lisäksi Hiltonin kuluja kasvatti heikkouksien korjaaminen sekä uusiin järjestelmiin panostaminen. (Stempel 2017.)

Yhtiöllä on yli 5100 kiinteistöä yli sadassa maassa ja siitä syystä Hilton onkin Skiftille antamassa tiedotteessaan vakuuttanut, että heillä on ollut laaja ja läpikotainen tutkinta tietomurrosta. Tutkinnassa Hilton Worldwide Holdings Inc:iä auttoi rikostekniset ammattilaiset, luottokorttiyhtiöt ja viranomaiset. Hilton on jatkossa sitoutunut suojaamaan asiakkaidensa luottokorttitietoja, jotta tinkimätön luottamus heidän järjestelmiinsä säilyisi. Tällaisten korvausten maksaminen tulevaisuudessa tulee mitä luultavimmin olemaan tavanomaista, sillä tämän kaltaiset tietomurrot ovat yleisiä. (Ting 2017.)

Hiltonin maksama 700 000 Yhdysvaltain dollaria korvauksia kuulostaa huomattavalta summalta, mutta se on vain kaksi dollaria per varastettu kohde. Mikäli tietomurrot olisivat tapahtuneet vuonna 2018, olisi maaliskuussa 2018 voimaan tullut GDPR eli Euroopan Unionin yleinen tietosuoja-asetus nostanut Hiltonin korvaussumman jopa 420 miljoonaan dollariin. Uuden tietosuoja-asetuksen mukaan korvattava summa voi olla jopa 4 prosenttia

yrityksen liikevaihdosta, joka Hiltonilla oli hyökkäyksen tapahtuessa vuonna 2014 10,5 Yhdysvaltain miljardia. (Roberts 2018.)

Hilton Worldwide Holdings Inc case toimii esimerkkinä siitä, minkälaisia rahallisia korvauksia yritys voi joutua maksamaan, mikäli tietomurtoja ei käsitellä oikein. Case esimerkistä käy myös ilmi taloudellisten vaikutusten ero, mikäli se olisi tapahtunut GDPR tietosuoja-asetuksen ollessa voimassa.

6 Tutkimus lähitulevaisuuden kyberuhista hotellialalla Suomessa

Tässä luvussa käymme läpi tutkimuksen tulokset opinnäytetyön rakenteen mukaisessa järjestyksessä sekä kerromme haastateltavien taustatiedot. Tutkimus suoritettiin laadullisena tutkimuksena teemahaastatteluja käyttäen. Teemahaastattelut toteutettiin eri tavoin, johtuen haastateltavien maantieteellisestä sijainnista tai anonymiteetin säilyttämisestä. Osa haastatteluista tehtiin anonyyminä, sillä haastattelut käsittelivät arkaluontoista tietoa. Anonyymeissä haastatteluissa haastateltavat itse vaativat anonymiteettiä. Osa haastatteluista ei olisi onnistunut, jos jo kysyttäessä ei olisi luvattu anonymiteettiä. Kysymykset teemoitettiin vastaamaan haastateltavien osaamisaluetta ja alaa. Haastattelun vastauksia peilataan hotellialan tulevaisuuden ja kybertoimintaympäristön teoriaan sekä case esimerkkeihin. Opinnäytetyön tarkoituksena on selvittää lähitulevaisuuden kyberuhat hotellialalla Suomessa. Työn tavoitteena on hyödyttää hotellialan toimijoita kyberuhkien tunnistamisessa. Lisäksi opinnäytetyön tavoitteena on luoda informatiivinen kooste niistä lähitulevaisuuden kyberuhkista, joita hotelliala tulee kohtaamaan. Tutkimuksen pohjalta rakennetaan malli, jonka tarkoituksena on auttaa hotellialan toimijoita kartoittamaan kyberuhat, joita ne omassa toiminnassaan lähitulevaisuudessa mahdollisesti kohtaavat.

Opinnäytetyöllä haetaan vastausta seuraavaan pääkysymykseen:

1. Millaisia kyberuhkia hotelliala Suomessa tulee kohtaamaan lähitulevaisuudessa?

Lisäksi haetaan vastausta seuraaviin alakysymyksiin:

2. Millaisia kyberuhkia teknologian kehitys hotellialalla tuo tullessaan?
3. Millaisia vaikutuksia kyberhyökkäyksellä on yritykseen?
4. Mitkä kansainväliset hotellialan kyberhyökkäykset todennäköisimmin leviävät Suomeen?
5. Mitkä toiminnot lähitulevaisuuden hotellissa ovat alttiimpia kyberuhille?

6.1 Haastattelut

Teemahaastatteluun valittiin asiantuntijat neljältä eri toimialalta. Valintaan vaikutti heidän kokemuksensa joko hotellialasta tai kyberturvallisuudesta. Haastatteluista kolme toteutettiin anonyymisti. Haastatteluista kaksi keskittyi hotellialaan ja kaksi kyberturvallisuuteen. Hotellialaan keskittyvät haastattelut olivat hotelli- sekä konsultointi- ja brändäysalalta. Kyberturvallisuuteen keskittyvät olivat kansainvälinen suunnittelualan konserni sekä tietotekniikka-ala. Hotellialaan keskittyviltä haastatteluilta toivottiin saatavan enemmän vastauksia liittyen hotellialaan, kun taas kyberturvallisuuteen keskittyvistä haastatteluista toivottiin

saavan enemmän kyberturvallisuuteen liittyviä vastauksia. Tutkimuksessa haastateltiin neljää eri asiantuntijaa neljältä eri alalta, jotta saatiin kattavat käsitys hotellialan muutoksesta sekä lähitulevaisuuden kyberuhista. Opinnäytetyön tekijät kokivat haastattelumäärän riittäväksi, sillä haastatteluista nousi jo nyt toistuvia teemoja esille.

Kuten edellä mainittiin, haastattelut toteutettiin puolistrukturoituina asiantuntijahaastatteluina, eli teemahaastatteluina. Tavoitteena oli luoda informatiivinen tuotos koskien lähitulevaisuuden kyberuhkia, joita hotelliala tulee kohtaamaan ja luoda niiden pohjalta malli. Haastattelut vastasivat erinomaisesti tavoitteita, jotka tutkimukselle oli asetettu. Haastatteluista nousi yhteneviä teemoja esille, jotka olivat pääosin linjassa tietoperustan kanssa. Haastattelujen avulla saatiin tietoja, jotka vastaavat opinnäytetyön pää- ja alakysymyksiin.

Asiantuntijat, joita opinnäytetyöhön haastateltiin, on esitelty alla.

1. **Johtaja suuressa Suomessa toimivassa hotellialan yrityksessä.** Hotellialan yrityksessä johtoasemassa toimiva henkilö valittiin haastateltavaksi tuomaan ammattilaisen näkemystä Suomen hotellialan tulevaisuudesta sekä kyberturvallisuuden nykytilasta. Haastateltavalla on laajaa kokemusta hotellialasta myös kansainvälisesti. Haastateltava valikoitui suosittelujen ja kontaktiverkostojen kautta tutkimukseen. Haastattelu toteutettiin teemahaastatteluna kasvokkain 18.10.2018. Haastattelu on käsitelty haastateltavan toiveesta anonyymisti, koska haastattelussa tuli ilmi arkaluontoisia tietoja Suomen hotellialaa koskien. Jatkossa haastateltavaan viitataan opinnäytetyössä nimellä haastateltava 1.

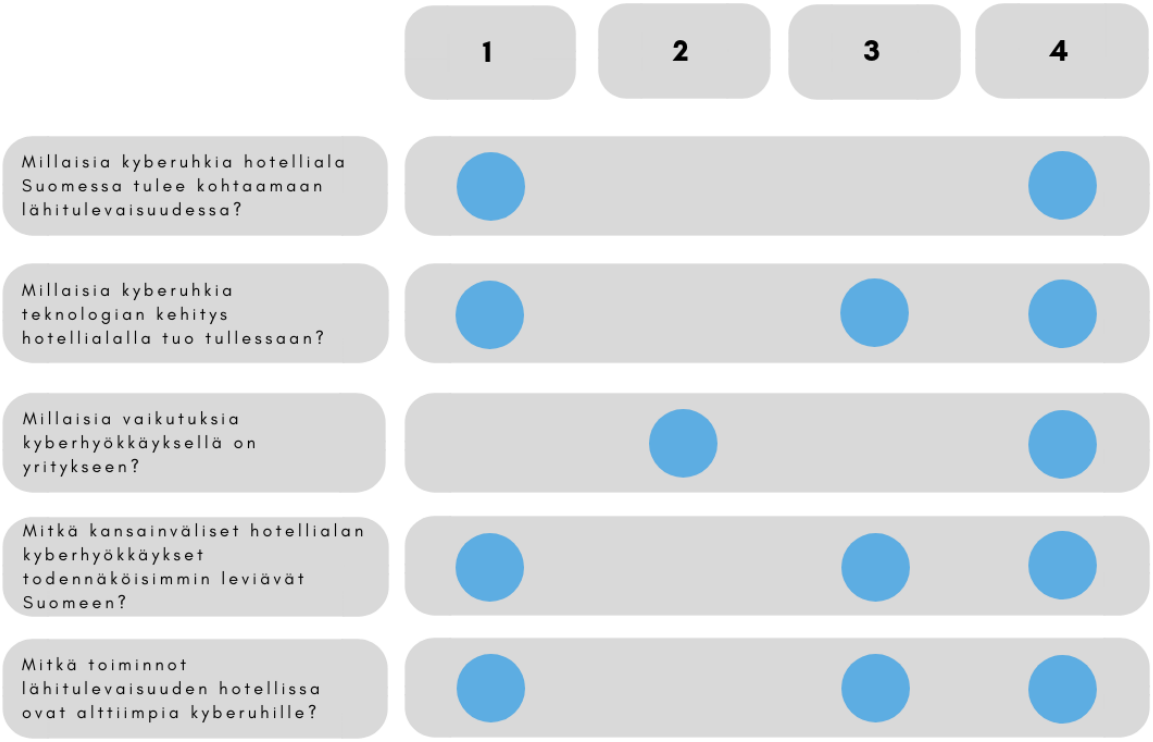
2. **Suuren kansainvälisen konsernin johtavassa asemassa oleva henkilö**. Haastateltava on opinnäytetyön tekijöiden kontakti. Haastateltava valittiin tutkimukseen, sillä yritys, jossa haastateltava on johtoasemassa, on viimeisen viiden vuoden aikana joutunut usean eri kyberhyökkäyksen sekä kyberhyökkäys yrityksen kohteeksi. Perille asti päässeitä kyberhyökkäyksiä yritykseen kohdistuen on ollut bottiverkkohyökkäys, joka sai yrityksen lamaantumaan täysin. Lisäksi yritys on kohdannut sähköpostikalastelun kautta tehdyn hyökkäyksen. Haastattelun tarkoituksena oli saada tietoa kyberhyökkäyksen aiheuttamista vaikutuksista yritykseen. Haastattelu toteutettiin teemahaastatteluna Skype for Business palvelun välityksellä puheluna 1.11.2018. Yritykseen kohdistuneet hyökkäykset eivät ole julkisessa tiedossa, mikä on peruste haastattelun anonyymiydelle. Jatkossa haastateltavaan viitataan opinnäytetyössä nimellä haastateltava 2.

3. **Matt Phillips johtaja ja perustaja Phillips & Co**. Yhdysvaltalaisessa yrityksessä. Phillips & Co. on konsultointialan yritys, jonka asiakkaita ovat muun muassa Hyatt- ja Starwood -hotelliketjut, Paramount Pictures sekä Archer -hotelli. Phillips & Co. luovat ja kehittävät uusia tuotteita, brändejä ja kasvustrategioita. Matt Phllipsin erikoisosaamista on innovaatiostrategiat, ideointi, tuotekehitys, brändistrategia sekä konseptikehitys ja –kokeilu. Phillipsin haastattelu keskittyi hotellialan tulevaisuuteen teknologian ja trendien näkökulmasta. Phillips tuntee Suomen hotellialaa jonkin verran, sillä hän on tehnyt yhteistyötä Haaga-Helian kanssa ja vierailee Suomessa tasaisin väliajoin puhumassa. Haastateltava on opinnäytetyön tekijöiden kontakti. Haastattelu toteutettiin sähköpostin välityksellä eri aikavyöhykkeiden vuoksi. Vastaukset haastatteluun saatiin 23.10.2018. Haastattelukielenä oli poiketen muista haastatteluista englanti. Jatkossa haastateltavaan viitataan opinnäytetyössä nimellä haastateltava 3.

4. **Turvallisuusalan yrityksessä toimiva hakkeri**. Hakkeria haastateltiin, jotta saatiin hyökkääjän näkökulmasta tietoa Suomen kyberturvallisuuden tilasta sekä sen tulevaisuudesta. Hakkeri tekee kyberhyökkäyksiä yrityksiin hyökkääjän näkökulmasta, jonka jälkeen hän kouluttaa henkilökuntaa tapahtuneista virheistä. Hakkeri valikoitui haastateltavaksi kontaktiverkostojen kautta. Hakkeria haluttiin haastatella opinnäytetyöhön, jotta ymmärretään myös hyökkääjän tapaa toimia ja näin ollen saada uutta näkökulmaa. Haastattelu suoritettiin teemahaastatteluna täysin anonyymisti Telegram –puheluna 31.10.2018. Hakkerin henkilöllisyys on tuntematon opinnäytetyön tekijöille, hänen yksityisyytensä turvaamiseksi. Jatkossa haastateltavaan viitataan opinnäytetyössä nimellä haastateltava 4.

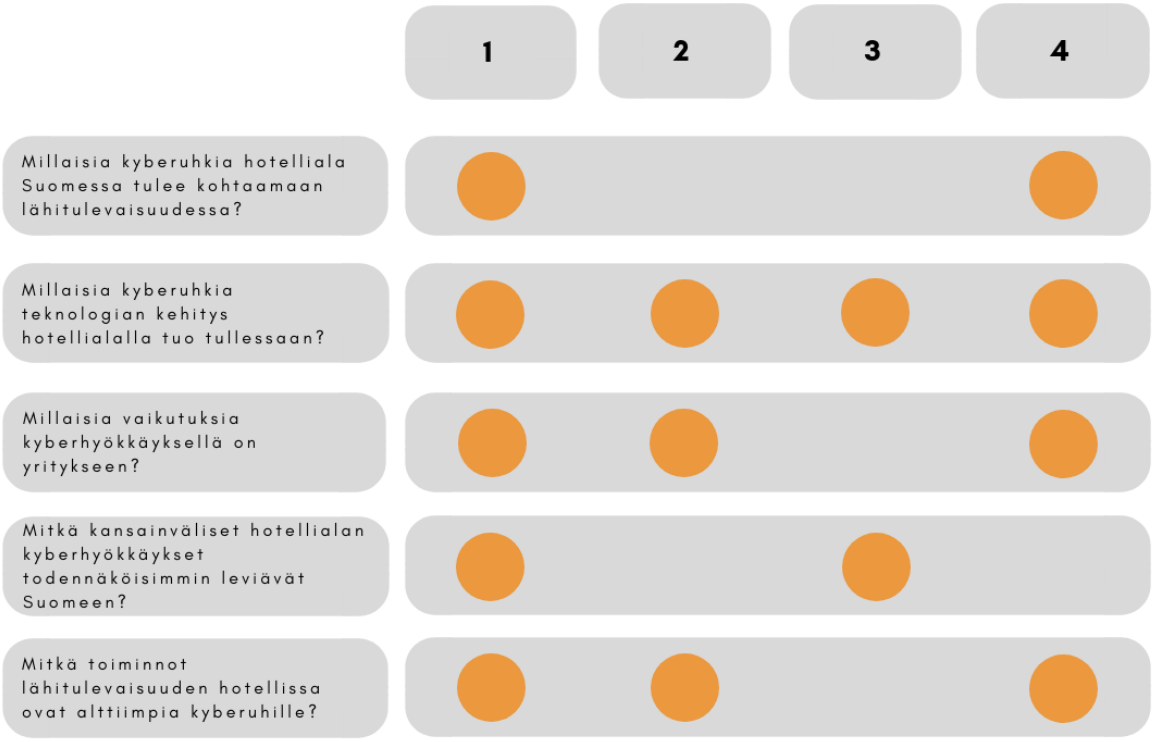
6.1.1 Teemahaastattelujen suunnittelu ja toteutus

Opinnäytetyön pääongelman ja tutkimuskysymysten pohjalta luotiin matriisi 1., joka määrittää mitä tietoja kultakin haastateltavalta haluttiin saada. Matriisin 1. oli myös tarkoitus auttaa haastattelukysymysten laatimista ja varmistaa niiden tarkoituksenmukaisuus. Haastattelujen toteutunut sisältö on kuvattu matriisissa 2. Haastattelujen kysymykset löytyvät liitteinä opinnäytetyön lopusta. Haastattelut teemoitettiin yhteneväisesti, mutta kaikille haastateltaville luotiin omat kysymykset.



Matriisi 1. Haastattelusisällön suunnitelma (Nenonen & Ojankoski 2018.)

Kun verrataan alkuperäistä ja toteutunutta suunnitelmaa keskenään, käy ilmi, että haastateltavilta 1 ja 2 saatiin vastaukset useampaan kysymykseen, kuin oli suunniteltu. Haastateltavilta 3 ja 4 taas saatiin vähemmän opinnäytetyön kysymyksiin vastauksia. Toteumasta näkyy myös epätasapaino kysyttyjen kysymysten ja saatujen vastausten määrän välillä. Tämä epätasapaino oli opinnäytetyön tekijöillä tiedossa, jonka vuoksi aihetta tutkittiin haastattelujen lisäksi kansainvälisten ja kotimaisten aineistojen avulla. Opinnäytetyön pää- ja alakysymyksiin on kaikkiin saatu vastaus.



Matriisi 2. Haastattelusisällön toteuma. (Nenonen & Ojankoski 2018.)

6.2 Hotellialan kyberturvallisuuden tila 2018

Tutkimuksessa selvisi, että hotellialan kyberturvallisuuden tila ei ole Suomessa toivotulla tasolla. Alalla tiedostetaan, että riskejä ja uhkia on, mutta niitä ei tunnisteta eikä niihin reagoida. Haastatteluista selvisi, että järjestelmät ovat vanhoja ja ne ovat kaikki kytketty samaan verkkoon, mikä heikentää niiden suojauskykyä. Haastateltava 4 kertoi yksinkertaisen verkon olevan yrityksen näkökulmasta riski. Jotta järjestelmät voitaisiin suojata tulisi jokainen järjestelmä kytkeä omaan verkkoonsa ja näin luoda kerrostettu suojaus.

Eniten käytössä olevia hotellivarausjärjestelmiä on Opera ja Hotellinx. Sen lisäksi käytössä on keskusvarausjärjestelmä Synxis, Trust ja Myfidelity sekä lukemattomia kanavanhallintajärjestelmiä. Kuten alaluvusta 4.3.2 tuli ilmi, on Synxis-keskusvarausjärjestelmän kautta tehty jo aiemmin laaja hyökkäys. Sabren Hospitality Solutions Synxis-keskusvarausjärjestelmään on hyökätty myös Trump hotellien hyökkäyksen jälkeen vuonna 2017. Hyökkäys koski jälleen heidän järjestelmien kautta tehtyjä hotellivarauksia. (Sabre 2017.) Hotellialalla käytössä on vanhaan tekniikkaan perustuvia järjestelmiä. Synxis, Trust ja Myfidelity keskusvarausjärjestelmien korvaaminen on aikaa vievää ja kallista, joten muutos on hidasta, mutta sitä tapahtuu. Uusia järjestelmiä kehitetään ja niitä myös yhdistyy.

Haastattelujen perusteella hotelleihin kohdistuvia kyberhyökkäyksiä tapahtuu päivittäin, mutta ne eivät tule julkisuuteen, sillä Suomessa asiasta ei ole tarvinnut ilmoittaa tähän mennessä. Haastateltavat 1 ja 2 kuitenkin uskovat tämän tulevan muuttumaan lähitulevaisuudessa uuden GDPR tietosuoja-asetuksen myötä.

> *”Nythän on niin, ettei Suomessa ole tarvinnut [kyberhyökkäyksistä] ilmoittaa. Meillähän [Suomen hotellialalla] tapahtuu päivittäin tällaisia asioita, mutta Suomen lain mukaan niistä ei tarvitse ilmoittaa. Jos vähän googlaillaan niin Jenkeissähän tarvitsee ilmoittaa, jos luottokorttitietoja viedään. Siellä on kohta kymmenen vuotta ollut sama käytäntö. Sen takia ei koskaan kuulla Suomesta, mutta kuullaan Amerikasta.” (Haastateltava 1, 18.10.2018.)*

Haastatteluista tuli ilmi, että tämän hetken suurin uhka on luottokorttitietojen varastaminen ja henkilö- sekä ostohistorian yhdistäminen muihin tietoihin. Haastateltava 1 näkee tämän hetken uhkana tietojen varastamisen. Harvoin hotellit kuitenkaan itse kohtaavat taloudellisia menetyksiä, sillä luottokorttiyhtiöt korvaavat asiakkaalle mahdolliset menetetyt varat.

Jokainen haastateltava koki kyberturvakoulutuksen riittämättömäksi omalla alallaan. Haastateltava 4, joka toimii hakkerina, kertoi että hyökkäykset ovat äärimmäisen helppo toteuttaa niin sanotusti alhaalta ylöspäin. Useimmiten hyökkäykset toteutetaan asiakasrajapinnassa olevan työntekijän kautta. Tämän lisäksi selvisi, että kyberturvakoulutuksia ei järjestetä, vaikka se koetaan tarpeelliseksi. Vastaukset ovat linjassa tietoperustan kanssa.

6.3 Hotellialan muutos

Hotellialan muutoksen tutkiminen oli välttämätöntä, jotta pystytään arvioimaan hotellialan tulevia kyberuhkia. Haastatteluissa keskityttiin hotellialan muutokseen pääosin teknologian näkökulmasta. Haastatteluissa sivuttiin myös trendejä, sillä ne ohjaavat muutosta. Haastattelujen lisäksi alan muutosta käsiteltiin opinnäytetyön teoriaosuudessa. Tässä alaluvussa aihetta käsitellään haastattelujen pohjalta.

Haastatteluissa toistuvasti nousi ilmi älyhotellit, lohkoketjut, älylukot, asiakkuuksien hallinta sekä isojen brändien merkitys tulevaisuudessa. Haastateltava 1 uskoo vahvasti lohkoketjuteknologian saapumiseen hotellialalle, kun taas haastateltava 4 oli epävarma sen käytöstä hotellialalla lähitulevaisuudessa. Haastateltava 4 epäili lohkoketjuteknologiaa, sillä hän ei usko sen hyödyttävän hotellialaa. Sen sijaan haastateltava 1 luottaa vahvasti, että lohkoketjuteknologia yksinkertaistaa ja keventää hotellijärjestelmiä sekä asiakkaanpolkua. Asiakkaiden tyytyväisyys nousi kantavaksi lähtökohdaksi monissa muutoksissa.

Muutoksia, jotka voidaan yhdistää asiakastyytyväisyyteen ovat älylukot, biometrinen tunnistus, henkilökohtaisuuden lisääntyminen ja asiakaspolun laajeneminen. Myös isojen yritysten tuleminen hotellialalle uudella tavalla nousi esille. Haastateltava 1 uskoo yritysten kuten Booking.com:in, Expedian ja Cventin tulevan tarjoamaan hotelleille kokonaisvaltaisia ratkaisuja. Näissä yritys tuottaa kaiken, kuten hotellivarausjärjestelmän, jakelun sekä revenue managementin. Esimerkkinä hän mainitsee Cvent kokous-, tapahtuma ja vieraanvaraisuusyrityksen, joka laajensi toimintaansa hotellioperoijaksi Accor Hotelsien kanssa. Haastateltava 3 taas uskoo isojen teknologiayritysten kuten Applen, Googlen ja Facebookin laajentavan toimintaansa hotellipuolelle. Isot yritykset laajentavat toimintaansa jatkuvasti aloille, joissa on paljon potentiaalia.

Kysyttäessä hotellihuoneiden lukitusjärjestelmistä ja niiden turvallisuudesta, tuli ilmi, että Suomessa ei ole edistyksellistä älylukkoteknologiaa käytössä haastateltava 1 mukaan. Hän kertoi Suomen hotellialan olevan tässä suhteessa vielä kovin perinteinen. Avaimet ovat pääsääntöisesti magneettijuovakortteja, Wingcardeja tai perinteisiä avaimia. Asiaan tarkemmin perehtyessä selvisi kuitenkin, että yhdessä pienessä yksityisessä hotellissa mobiiliavaimet ovat otettu jo käyttöön. Kuten alaluvussa 3.4 kerrottiin, on Hoist Groupin tarjoama mobiiliavain käytössä jo Hiisi Homes & Hotels Helsinki Haaga-hotellissa. Suomesta ei myöskään löydy paljoa muuta pitkälle vietyä huoneteknologiaa haastateltava 1 mukaan. Hänen mukaansa St.George hotellissa on otettu jo kevyesti käyttöön huoneautomaatioita.

> *”St.Georgessa on pisimmälle viety huoneautomaatio, missä pystyy tiettyjä asioita säätämään itse siellä huoneessa, mutta ne ovat silti hyvin perinteisiä. Niitä ei pysty ohjaamaan millään sovelluksella.” (Haastateltava 1, 18.20.2018.)*

Haastateltava 3 uskoo Suomeen tulevan innovatiivisia ja luovia ratkaisuja hotelleihin. Hotelliala on hänen mukaan Suomessa jäljessä, kun verrataan Yhdysvaltoihin, tämä johtuu erosta väkimäärässä. Teknologian ja älyhotellien lisääntymistä pidetään varmana, mutta kaikista hotelleista ei kuitenkaan uskota tulevan älyhotelleja. Hänen mukaansa bisnes- ja konferenssihotelleissa asiakkaat toivovat paljon automatisoituja ratkaisuja. Haastateltava 3 näkee tilanteen niin, että tarjoama hotellien osalta vain laajenee. Hän uskoo, että teknologisia ratkaisuja tullaan näkemään entistä enemmän. Esimerkkinä hän mainitsee robotiikan sekä uudet tavat maksaa. Haastateltava 3 mielestä Aasia on tässä suunnannäyttäjä. Aasiassa biometristä tunnistusta on alettu jo hyödyntää hotellialalla maksutapana, kuten alaluvusta 3.4 selviää.

” In every market there are always different kinds of products. It’s likely that in the future hotels will be like cars today – some are still very basic and some can drive themselves. Hotels will change, but will still serve a wide range of needs and price points.” (Haastateltava 3. Phillips, 23.10.2018.)

6.4 Lähitulevaisuuden kyberuhat

Kaikissa haastatteluissa keskityttiin lähitulevaisuuden kyberuhkiin. Puolet haastatteluista keskittyivät hotellin näkökulmaan ja toinen puoli yleisesti tuleviin kyberuhkiin. Yhteneviä teemoja löytyi kuitenkin kaikista haastatteluista. Esille nousseita uhkia, joista lähes kaikki haastateltavat olivat yhtä mieltä, oli henkilöstön kyberkouluttamattomuus, rahalliset menetykset ja riskialttiit järjestelmät sekä -verkot. Haastattelujen perusteella kyberhyökkäysten suurin motivoiva tekijä on ja tulee olemaan raha.

Haastatteluista jo aiemmin ilmi tullut henkilöstön kyberkouluttamattomuus tulee olemaan alati kasvava riski. Lähes kaikki haastateltavat kokivat tämän suurimmaksi uhaksi. Tämä perustuu heidän omiin tietoihinsa ja kokemuksiinsa kyberhyökkäysten määrän kasvusta, jolloin kyberkouluttamaton henkilökunta ei ole varautunut kohtaamaan näitä uhkia. Haastateltava 4 kertoo asiakasrajapinnassa olevien työntekijöiden olevan helpoin hyökkäyksen kohde, sillä juuri he eivät usko joutuvansa kyberhyökkäyksen kohteeksi. Hänen mukaansa tämä mahdollistaa hyökkäyksen, jossa otetaan kohteen sähköposti haltuun ja sen avulla kalastellaan tietoja tai asennetaan haittaohjelmia. Tällaisin keinoin päästään käsiksi yhä tärkeämpiin tietoihin. Tämän kaltaiset hyökkäykset ovat trendikkäitä hakkerien keskuudessa. Haastateltava 4 pitää tätä todennäköisenä hyökkäystapana myös tulevaisuudessa sen helppouden vuoksi. Haastateltava 2 on tästä yhtä mieltä, sillä osa heidän yritystään kohdanneista kyberhyökkäyksistä on tehty sähköpostin haltuunoton kautta.

” Kiristyshän siellä on taustalla, eli lähdettiin kiristämään, että jos maksatte Bitcoineja, niin vapautamme teidän serverit ja muut tiedot. Mikä se Bitcoinien määrä kokonaisuudessaan on ollut, niin se on varmaan ollut valtava. Ei me siihen lähdetä.” (Haastateltava 2, 1.11.2018.)

Haastateltava 2 uskoo tämän kaltaisten hyökkäysten lisääntyvän tulevaisuudessa. Haastateltavat 2 ja 4 olivat yhtä mieltä myös siitä, että tämän kaltaisten hyökkäysten perimmäisenä tarkoituksena on lamauttaa hyökkäyksen kohteen järjestelmät alas ja vaatia lunnaita niiden palauttamiseksi. Hyökkäys voidaan toteuttaa joko tietojen kalasteluna tai sähköpostin kautta lähetettävinä liitetiedostoina, jotka sisältävät haittaohjelmia. Haastateltava 2

epäilee hyökkäysten kokonaiskustannusten nousevan miljooniin euroihin. Kustannukset koostuvat palkkakustannuksista sekä menetetystä liikevaihdosta, mikäli asiakkaalta ei voida veloittaa työtunneista. Työtunteja joudutaan käyttämään moninkertaisesti verrattuna budjetoituihin tunteihin, joka hidastaa työn suorittamista. Hänen mukaansa paras sijoitus on ennakkovarautuminen, jolloin palautuminen hyökkäyksistä on nopeampaa ja aiheuttaa yritykselle vähemmän kuluja. Lisäksi hän listaa toipumissuunnitelman ja henkilöstön kouluttamisen tärkeiksi sijoituksiksi.

Maineen menetystä kyberhyökkäyksen seurauksena ei tällä hetkellä koeta riskiksi. Tämä johtuu siitä, että yrityksen ei vielä julkisesti tarvitse ilmoittaa hyökkäyksistä. Haastateltavat kuitenkin uskovat tämän tulevaisuudessa olevan riski, sillä EU:n GDPR tietosuoja-asetus tulee vaikuttamaan ilmoitusvelvollisuuteen. Haastateltava 4 näkee tämän selkeänä uhkana jo nyt. Vaikka ilmoitusvelvollisuutta ei vielä ole, voidaan kuitenkin mainetta vahingoittaa myös monilla muilla tavoin. Esimerkkinä hän mainitsee osakkeiden julkistamisen, joka johtaa arvon laskuun ja sen johdosta yrityksen maine kärsii, mikäli se ei maksa lunnasvaatimuksia. Kuten alaluvusta 4.2 selviää, on maineen menetys kansainvälisesti hotellialalla yksi suurimmista kyberuhista.

Haastatteluissa nousi esille edistyksellisen teknologian riskit. Haastateltavat kokevat, että mitä edistyksellisempää teknologia on, sitä suurempi riski siihen sisältyy. Haastateltava 1 kertoi, että Suomessa ei vielä ole tämän kaltaista teknologiaa, lukuun ottamatta uutta St.George hotellia, jossa osan huonesäädöistä voi tehdä itse. Kuitenkin haastateltavat 1 ja 3 uskovat älyhotellien yleistyvän. Älyhotellien yleistyminen lisää käytettäviä teknologioita. Haastateltavat olivat lähes yhtä mieltä siitä, että teknologisten ratkaisujen lisääntyessä syntyy uusia kyberuhkia. Haastateltava 3 uskoo silti turvallisuuden lisääntyvän teknologian myötä.

> *” Hotel industry is becoming more resilient. The amount of information hotel managers and owners have now about their facilities and guest perception of their properties in unprecedented. Information is the key to maintaining and improving almost anything.” (Haastateltava 3, Phillips, 23.10.2018.)*

Haastateltava 4 on taas sitä mieltä, että mitä useampi tällainen teknologinen ratkaisu otetaan käyttöön, sitä useampi väylä murtautua järjestelmiin on. Tällaisia teknologisia ratkaisuja on esimerkiksi citizenM hotelleissa jo käytössä oleva moodpad-huoneautomaatio. Haastateltava 4 pitää lunnasvaatimushyökkäyksiä kuitenkin kannattavimpana ja hyökkää-

jän kannalta riskittömimpänä hyökkäyksen muotona, sillä ne voidaan tehdä etänä salattujen verkkojen kautta. Paikan päällä tapahtuva murtautuminen järjestelmiin hotellin verkon kautta ei ole hänen mukaansa houkuttelevaa, sillä siihen liittyy suurempi riski.

Haastatteluista ilmeni, että asiakkaaseen ja asiakaspolkuun tullaan kiinnittämään nykyistäkin enemmän huomiota. Asiakkaista tullaan keräämään entistä enemmän tietoa muun muassa CRM-järjestelmään ja koko asiakaspolku pyritään laajentamaan. Asiakkaista pyritään keräämään tietoa, jotta heitä pystyttäisiin palvelemaan tehokkaasti jo ennen matkan suunnittelua sekä matkan jälkeen. Haastatteluissa tuli esille myös ostokäyttäytymisen muuttuminen, mikä tulee muovaamaan sitä, minkälaisissa hotelleissa tulevaisuuden asiakkaat tulevat majoittumaan. Näiden muutosten vuoksi haastateltava 3 uskoo CRM-järjestelmän tekevän entistä tehokkaampaa ja parempaa työtä kerätessään asiakkaista tietoa. Tämä sen vuoksi, että tekoäly pystyy muovaamaan asiakaskokemuksen henkilökohtaisemmaksi. Kokonaisvaltaisempi asiakasprofiili on haastateltava 4 mielestä houkutteleva hakkeroinnin kohde, jonka kautta voidaan vaatia lunnaita. Hänen mukaansa kaikki pitkään kerätty ja käsin kasattu tieto on yritykselle korvaamatonta, josta johtuen yritykset ovat valmiita maksamaan vaaditut lunnaat tietojen palauttamiseksi.

Lohkoketjuteknologia jakoi mielipiteitä haastateltavien välillä. Toisaalta se koettiin hotellialaa muuttavana asiana, kun taas toisaalta ei ymmärretty mitä hyötyjä se toisi alalle. Haastateltava 1 kokee lohkoketjuteknologian asiana, joka tulee hotellialalle ja muuttaa tiedon siirtämiseen, turvallisuuteen ja maksamiseen liittyviä seikkoja. Haastateltava 2 ei toistaiseksi ole törmännyt omalla alallaan lohkoketjuteknologiaan, mutta uskoo, että siitä voisi olla hyötyä. Esimerkiksi hän antaa heidän yritykseensä kohdistuneen hyökkäyksen, jossa pelastuneet tiedot olivat pilvipalveluissa ja menetetyt tiedot omilla servereillä. Haastateltava 4 ei nähnyt hotellialan hyötyvän lohkoketjuteknologiasta juuri ollenkaan, jonka takia hän ei usko sen tulevan käyttöön.

Kysyttäessä biometrisestä tunnistuksesta, siihen uskottiin liittyvän riskejä, sillä esimerkiksi haastateltava 4 näkee sen vielä alkeellisena. Alkeellisuuden vuoksi väärinkäyttöjä on helppo tehdä ja järjestelmiä huijata. Teoreettisen tutkimuksen perusteella biometrinen tunnistus tulee osaksi hotellialaa tulevaisuudessa, vaikka haastateltavat eivät nostaneetkaan sitä todennäköisimmäksi muutokseksi.

7 Yhteenveto ja johtopäätökset

Tässä luvussa tuodaan esille johtopäätökset ja tehdään yhteenveto. Yhteenveto perustuvat hotellialan muutokseen, Suomen ja kansainväliseen kyberturvallisuuden tilaan sekä asiantuntijoiden haastatteluihin. Opinnäytetyön tavoitteena oli tutkia mitä kyberuhkia hotelliala Suomessa tulee kohtaamaan. Tavoitteena oli luoda informatiivinen kooste koskien lähitulevaisuuden kyberuhkia, joita hotelliala tulee kohtaamaan. Tutkimuksen pohjalta luotiin malli, jonka tavoitteena on auttaa hotellialan toimijoita kartoittamaan kyberuhat, joita ne mahdollisesti kohtaavat lähitulevaisuudessa omassa toiminnassaan.

Hotelliala kohtaa Shabanin (2016, 9.) mukaan tällä hetkellä viisi eri kyberuhkaa, joita ovat luottokorttitietojen varastaminen, uhka-analyysin ja turvallisuusauditointien puute, kilpailuedun menettäminen, fyysiset rikokset, jotka asettavat hotellin vaaraan, ja langattoman verkon kautta tehdyt hyökkäykset. Tietoperustan ja haastattelujen perusteella Suomessa hotellialan viisi suurinta kyberuhkaa lähitulevaisuudessa ovat henkilö- sekä luottokorttitietojen menettäminen, lunnasvaatimukset, verkon ja langattoman verkon kautta tapahtuvat hyökkäykset sekä maineen menettäminen. Monet verkon ja langattoman verkon kautta tehtävät hyökkäykset ovat haittaohjelmia.

Hyökkäyksistä aiheutuu lähes aina taloudellisia vaikutuksia, mistä syystä kyberuhkien tiedostaminen ja niihin varautuminen on hotelleille tärkeää. Hyökkäysten motivaationa on lähes aina raha, johtuivat hyökkäykset sitten kiristyksestä tai luottokortti- ja henkilötietojen varastamisesta. Accenturen (2017, 20, 27.) mukaan kyberhyökkäyksistä aiheutuvat kulut ovat nousseet jopa 23 prosenttia kansainvälisesti. Vieraanvaraisuusalalla kulut ovat 5,04 miljoonaa Yhdysvaltain dollaria vuodessa. Suurimmat yksittäiset kulut hyökkäyksissä johtuvat datan ja informaation menetyksestä, jotka toistuvuudellaan ovat nousset 35 prosentista 45 prosenttiin. Teoriaa tutkiessa selvisi, että suojauksiin käytettyä rahaa ei osata kohdistaa oikeisiin toimintoihin. Tätä väitettä tukevat myös haastattelut, joissa muun muassa ilmeni, että henkilöstöä ei kouluteta juuri ollenkaan. Haastateltava 2 arvioi omaa yritystään kohdanneiden hyökkäysten kustannusten nousseen miljooniin. Hänen mukaansa tämä olisi mahdollista välttää ennakkovarautumisella, palautumissuunnitelmalla sekä henkilöstön kouluttamisella.

Nykytilaa tutkittaessa saatiin selville, että älyteknologian osalta hotelliala Suomessa on perinteinen verrattuna kansainväliseen hotellialaan. Sekä haastattelujen, että tietoperustan (Raeste 2018.) mukaan käy ilmi, että Suomessa ei ole älyhotelleja eivätkä seuraavienkaan vuosien hankkeet anna vielä viitteitä, että sellaisia olisi tulossa. Haastateltavat kui-

tenkin uskovat älyhotellien rantautuvan jossain vaiheessa Suomeen. Sen sijaan muita teknologisia ratkaisuja otetaan käyttöön lähivuosina. Analysoitaessa hotellialan tulevaisuutta, todettiin tietoperustassa, että Suomessa hotelliala kasvaa tasaisesti. Aution (2017.) mukaan markkinat houkuttelevat uusia investoijia. Tästä voidaan päätellä hotellialan kasvun ja uusien investoijien tuovan Suomeen uusia hotellitrendejä. Kansainvälisten konferenssien määrä ja Helsingin potentiaali konferenssien järjestäjänä on kasvussa. Haastateltava 3 mukaan bisnes- ja konferenssiasiakkaat haluavat paljon automatisoituja ratkaisuja. Näillä perusteilla voidaan tehdä johtopäätös, että teknologisille ratkaisuille on kysyntää lähitulevaisuudessa. Myös aasialaisten matkailijoiden määrän kasvu voi indikoida teknologian tarvetta, koska Aasiassa teknologiset ratkaisut on viety jo pidemmälle.

Haastatteluissa todettiin henkilökohtaisuuden, uusien maksutapojen, teknologisten ratkaisujen ja robotiikan lisääntyvän. Tietoperustassa tätä tukee TrendWatchingin (2017.) ja Skiftin (2018, 33, 53, 57, 62.) ennusteet megatrendeistä, joita ovat yksilön tärkeyden korostuminen, ihmisen tarve olla yhteydessä, kasvava informaation nälkä, älylaitteiden merkityksen kasvu ongelmanratkaisijoina sekä kokonaisvaltainen palvelutarjoama. Opinnäytetyössä on megatrendejä ja teknologian kehitystä kuvattu esimerkkien kautta, jotka ovat citizenM -hotelliketju sekä Hen Na hotelli Tokiossa. Esimerkiksi Henn Na hotellissa on käytössä robotiikkaa ja biometrinen tunnistus.

Suomessa ei huoneautomaatio haastattelujen mukaan ole vielä kovinkaan pitkällä, mutta uusien innovatiivisten ratkaisujen uskotaan lisääntyvän. Todennäköistä on, että huoneautomaation käyttö ja tätä kautta henkilökohtaisuuden lisääminen hotelleissa kasvaa. Tästä antaa viitteitä myös Suomessa jo Radisson Blu:lla käytössä oleva One Touch –sovellus. (Radisson Blu 2018.) Opinnäytetyön esimerkissä citizenM hotelleissa uusinta teknologiaa edustaa moodpad-huoneautomaatioteknologia, jolla henkilökohtaisuutta korostetaan hotellin majoituksessa. Tietoperustassa megatrendiksi nimettiin yksilön tärkeyden korostuminen ja haastattelut tukivat tätä teoriaa. Haastateltavat uskovat teknologian lisääntyvän hotelleissa, jota tukee myös teoriaosuudessa esitelty mobiiliavain, joka on Suomessa otettu käyttöön jo ainakin yhdessä hotellissa.

Älykkään teknologian lisääntyminen hotelleissa, tuo mukanaan uusia uhkia ja tietoturvariskejä. Esimerkiksi älylukkojen käyttöönotto voi tuoda mukanaan lunnasvaatimukset, jolloin hotellin lukitusjärjestelmät otetaan hakkerien toimesta haltuun esimerkiksi haittaohjelman avulla ja niiden vapauttamiseksi vaaditaan lunnaita. Haastateltava 4 kertoi lunnasvaatimushyökkäyksen olevan todennäköisempi, sillä hyökkääjä voi toteuttaa hyökkäyksen etänä, kun taas järjestelmiin murtautuminen hotellin verkon kautta paikan päällä on hyök-

kääjälle riskialttiimpaa. Tämä uhka on jo toteutunut itävaltalaisessa Seehotel Jägerwirtissä, jossa vieraat lukittiin ulos huoneistaan. Haastatteluista ilmeni älylaitteisiin liittyvä riski, jossa luottokorttitiedot on mahdollista viedä murtautumalla älylaitteen kautta hotellin järjestelmiin. Edellä mainittujen lisäksi tietoperustasta selviää, että asiakkaan kaikki tiedot voidaan varastaa niin kutsutun välikäden kautta, jolloin asiakkaan puhelimeen tai älylaitteeseen päästään käsiksi, kun asiakas kirjautuu hotellin langattomaan verkkoon. (Kevin Davis Insurance Services 2018)

Haastatteluissa biometrinen tunnistus ei noussut erityisemmin esille kysyttäessä hotellialan teknologian muutoksesta. Yhdessä haastattelussa kuitenkin todettiin, että uusissa maksutavoissa Aasia on suunnannäyttäjä. Henn Na hotelli toimii tästä hyvänä esimerkkinä, sillä hotellin toiminta perustuu biometriseen tunnistukseen ja robotiikkaan. Henn Na hotelli on käytännöllinen ja moderni sekä tarjoaa korkeatasoista teknologiaa. Kuten tietoperustasta selviää, on Bulgariassa ja Etelä-Afrikassa sormenjäljellä toimivat maksukortit jo käytössä. Aasiaan tätä teknologiaa yhdessä kasvojen tunnistuksen kanssa on markkinoille tuomassa MasterCard. Tietoperustassa Kobresin (2018.) ja DigFinin (2018.) mukaan biometrinen tunnistus muokkaa maksu- ja hankintaprosesseista entistä saumattomampia. Tämän vuoksi voidaan olettaa, että tulevaisuudessa vastaavanlaista teknologiaa otetaan käyttöön myös Suomessa. Biometrisen tunnistuksen mukanaan tuomia uhkia on järjestelmän huijaaminen ja väärinkäyttö, sillä kuten haastatteluista selviää, on se vielä alkeellista. Tästä johtuen asiakkaan luottokorttitietoja voidaan väärinkäyttää sekä heidän henkilötietojaan varastaa.

Dogru ym. (2018, 2-5.) uskovat lohkoketjujen käyttöönoton lisääntyvän. Lohkoketjuteknologian avulla maksut, rahansiirrot ja varaukset helpottuisivat. Heidän mukaansa lohkoketjuteknologia olisi hyödyllinen ja turvallinen, mutta sisältyy siihen Biswasin & Santhanan (2017, 5-6.) mukaan riskejä. Haastatteluissa lohkoketjuteknologia jakoi mielipiteitä, sillä osa koki sen osana tulevaisuutta, kun taas osa näki sen hyödyt, mutta ei ollut kuullut sen käytöstä. Hakkerina toimiva haastateltava 4 ei nähnyt lainkaan sen hyötyjä hotellialalla. Hotellialan ammattilaista haastateltaessa (haastateltava 1.) se nähtiin tärkeänä osana hotellialan tulevaisuutta, joka tuki tietoperustaa. Tietoperustassa Biswasin & Santhanan mukaan lohkoketjuteknologian riskejä olivat pääsy suljettuun lähdekoodiin ja tästä johtuva asiakkaiden henkilötietojen menettäminen tai luvattomien siirtojen tekeminen. Murtautuminen suojattuun lähdekoodiin on riski, sillä silloin hyökkääjä pääsee käsiksi asiakastietoihin, mahdollisuuteen tehdä ilman välittäjää toimivia siirtoja ynnä muihin tietoihin. Tietoperustassa ilmenee, että huonosti toimiva lohkoketjuteknologia voi johtaa negatiiviseen asiakaskokemukseen, mikäli perusrakenne ei sovi saumattomasti yhteen hotellin järjestelmien

kanssa. Negatiiviset asiakaskokemukset voivat pidemmän päälle johtaa maineen menettämiseen.

Haastatteluista tuli esille, että henkilöstöä ei kouluteta kyberturvallisuudesta tarpeeksi tai ollenkaan. Lähes kaikki haastateltavat nostivat kyberkouluttamattoman henkilökunnan suurimmaksi riskiksi. Tätä tukee tietoperustassa Bradford (2018.), jonka mukaan hakkerit luottavat enemmän ihmisten tekemiin virheisiin, kuin tietoturva-aukkoihin, jonka vuoksi kouluttaminen ja kouluttautuminen ovat järkeviä keinoja vähentää kyberuhkien riskejä. Esimerkki onnistuneesta koulutuksesta on case Bangladesh Central Bank ja New York Federal Reserve Bank, jossa työntekijän valppauden vuoksi estettiin mittavat taloudelliset vahingot. Tietoperustan ja haastattelujen pohjalta voidaan siis päätellä, että kyberkouluttamaton henkilökunta aiheuttaa kasvavissa määrin kyberuhkia yrityksille. Kyberkouluttamattomasta henkilökunnasta johtuvia uhkia ovat verkkohyökkäykset, joita tehdään sähköpostin kautta sekä järjestelmät lamauttavat hyökkäykset, joiden tarkoituksena on vaatia lunnaita ja kiristää siten rahaa yritykseltä. Kyberkouluttamaton henkilökunta voi johtaa asiakkaiden luottokorttitietojen menetykseen, mikäli he eivät tunnista epäilyttävää tai pahantahtoista toimintaa. Hakkerit luottavat inhimillisiin virheisiin, joka todetaan myös tietoperustassa. Tietoperustassa Disparten & Furlown (2017.) mukaan kouluttamisella pystytään säästämään suuria summia rahaa.

Haastatteluista ilmeni kyberhyökkäyksiä tapahtuvan hotellialalla päivittäin. Haastatteluista ja tietoperustasta selviää, että nämä eivät kuitenkaan tule julkisesti ilmi, sillä Suomen lainsäädännössä komission asetus (EU) N:o 611/2013 ei velvoita ilmoittamaan niistä. Kahdessa haastatteluista tämä nostettiin kuitenkin seikaksi, joka tulevaisuudessa tulee muuttumaan uuden GDPR tietosuoja-asetuksen myötä. Yhdessä haastattelussa todettiin (Haastateltava 1, 18.10.2018.), että tulevaisuudessa tullaan siirtymään malliin, jossa hyökkäyksistä tulee ilmoittaa julkisesti. Tämä voi johtaa suuriin korvauksiin, mikäli hyökkäyksiä ei käsitellä oikein. Esimerkkinä tästä toimii Hilton Hotelseihin kohdistunut tietomurto, jossa korvattava summa olisi noussut 420 miljoonaan dollariin (4% yrityksen silloisesta liikevaihdosta), mikäli hyökkäys olisi tapahtunut Euroopassa GDPR:n ollessa voimassa. Muita tämän tuomia uhkia ovat maineen menettäminen johtuen ilmoitetuista hyökkäyksistä sekä heikentynyt kilpailuetu maineen ja taloudellisten menetysten takia.

Tulevaisuudesta puhuttaessa haastatteluissa nousi esille asiakasprofiilien sekä CRM-asiakastietojärjestelmien tietomäärän kasvu. Tulevaisuudessa asiakkaasta tullaan keräämään entistä tarkemmin tietoa ja sen avulla voidaan asiakaskokemusta muokata henkilökohtaisemmaksi. Tästä voidaan päätellä, että mitä enemmän asiakkaista kerätään tietoa,

sitä arvokkaampaa se on hotellille ja sitä alttiimpi kyberhyökkäyksille. Tätä tukee tietoperustassa oleva case esimerkki The Trump Hotel Collectionista, jossa asiakkaiden henkilökohtaisia tietoja vietiin hyökkäyksen seurauksena. Jo aiemmin todetusti laaja asiakasprofiili on arvokas ja houkutteleva kohde hyökkääjille. Yksi hyökkäystapa on kaapata asiakasprofiilit ja vaatia niiden palauttamisesta lunnaita, perustuen niiden tärkeyteen hotellille. Mikäli nämä tiedot menetetään hyökkäyksen seurauksena, aiheuttaa se maineen heikentymistä. Tämän vuoksi laaja asiakasprofiili tuo mukaan kyberuhkia.

Teorian ja haastattelujen perusteella hotellialalla Suomessa suuria muutoksia ovat:

1. Älylaitteet ja –lukot
2. Laaja asiakasprofiili
3. Lohkoketjuteknologia
4. GDPR eli EU:n yleinen tietosuoja-asetus
5. Kyberkouluttamaton henkilökunta
6. Biometrinen tunnistus

Muutoksia koskevat todennäköisimmät kyberuhat:

1. Luottokorttitietojen menettäminen
2. Asiakkaiden henkilötietojen menettäminen
3. Lunnasvaatimukset
4. Maineen menettäminen
5. Verkkohyökkäykset
6. Langattoman verkon kautta tapahtuvat hyökkäykset
7. Rahalliset korvaukset
8. Murtautuminen suljettuun lähdekoodiin
9. Järjestelmien huijaaminen ja väärinkäyttö
10. Kilpailuedun menettäminen

Nämä kuusi muutosta ja kymmenen muutoksia koskevaa kyberuhkaa ovat pohjana lähitulevaisuuden kyberuhkamallin luomisessa. Näihin tuloksiin päästiin peilaamalla haastattelujen vastauksia tietoperustassa olevaan teoriaan.

7.1 Malli lähitulevaisuuden kyberuhista

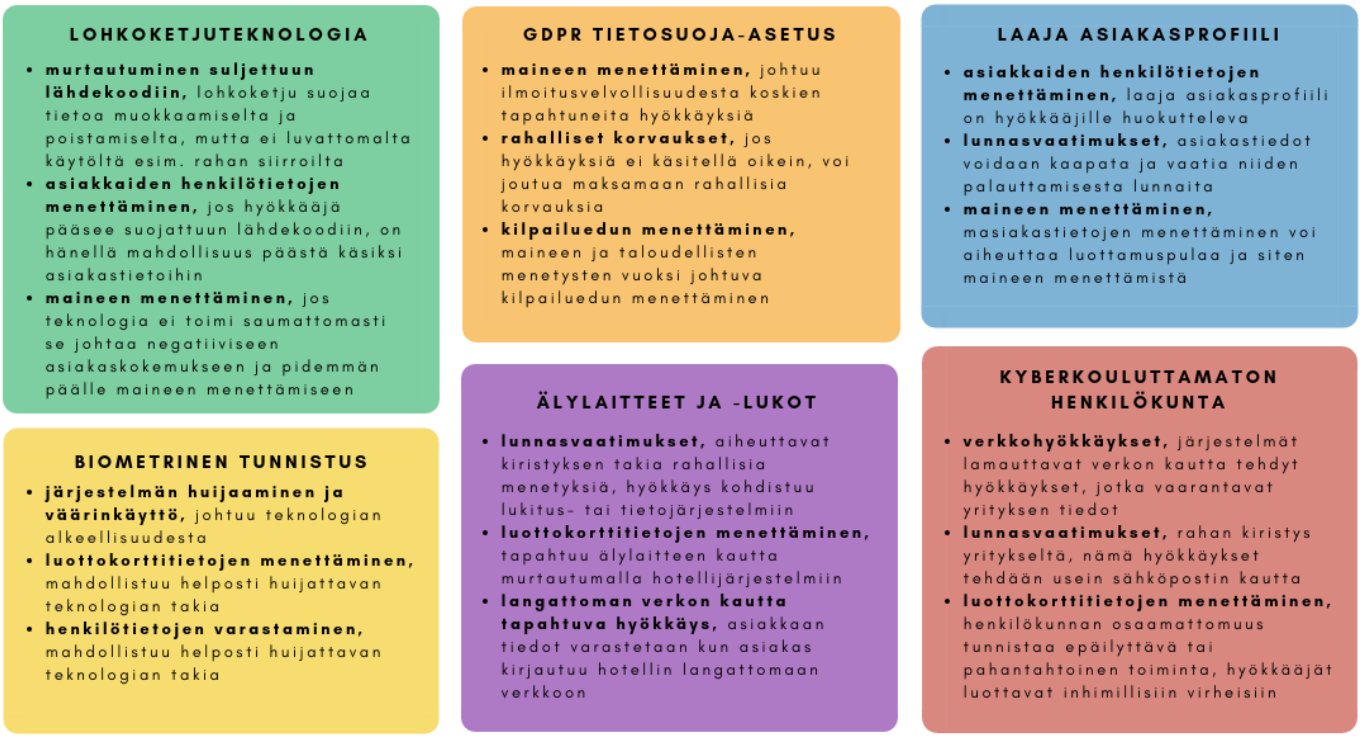
Tässä alaluvussa esitellään Kyberuhkien Kartoituksen Kidemalli, joka on luotu teorian ja tutkimuksen pohjalta auttamaan hotellialan yrityksiä kartoittamaan lähitulevaisuuden kybe-

ruhkia. Mallin tarkoituksena on auttaa hahmottamaan mitä uhkia hotelli lähitulevaisuudessa kohtaa, sen perusteella mitä uusia toimintoja hotellissa on otettu käyttöön. Opinnäytetyön tavoitteena oli luoda informatiivinen tuotos koskien lähitulevaisuuden kyberuhkia, joita hotellia tulee kohtaamaan. Malliin on valittu hotellialan todennäköisimmät muutokset lähitulevaisuudessa, joiden perusteella nähdään mitä kyberuhkia muutos tuo tullessaan. Nämä uhat ovat valikoituneet malliin tutkimuksen perusteella. Suurin uhka on kuvattu tummimmassa osiossa, kun taas vaaleimmassa osiossa on vähiten todennäköinen uhka todennäköisistä uhista.

Kuvio 4. Malli lähitulevaisuuden kyberuhista hotellialalla Suomessa. (Nenosen & Ojankosken Kyberuhkien Kartoituksen Kidemalli 2018.)

Kyberuhkien Kartoituksen Kidemallia käytetään niin, että ensimmäisenä valitaan omaa hotellia koskevat muutokset isoimmista kuusikulmaisista kohdista, kohtia on yhteensä kuusi.

Jokaista muutosta kohden on kolme todennäköisintä kyberuhkaa. Tämän jälkeen nähdään mitkä kyberuhat koskevat kohdehotellia. Kyberuhkien Kartoituksen Kidemallin toinen osa on selvitysosa, joka avaa hieman uhkia ja helpottaa niiden ymmärtämistä. Selvitysosassa selitetään miksi kyseinen uhka koskettaa kyseistä muutosta. Muutoksia koskevia kyberuhkia on yhteensä kymmenen, mutta ne aiheutuvat eri syistä ja vaikuttavat eri tavoilla riippuen muutoksesta.



Kuvio 5. Malli lähitulevaisuuden kyberuhista hotellialalla Suomessa osa 2. (Nenosen & Ojankosken Kyberuhkien Kartoituksen Kidemallin selvitysosa 2018.)

8 Pohdinta

Opinnäytetyön tavoitteena oli tutkia mitä kyberuhkia hotelliala Suomessa tulee kohtaamaan. Tavoitteena oli myös luoda informatiivinen kooste hotellialan lähitulevaisuuden kyberuhkista. Tutkimuksen pohjalta oli tarkoitus luoda malli, jonka tavoitteena on auttaa hotellialan toimijoita kartoittamaan kyberuhat, joita ne mahdollisesti kohtaavat lähitulevaisuudessa omassa toiminnassaan. Edellä mainitut tavoitteet täytettiin erinomaisesti. Opinnäytetyön tekijöiden mielestä rajatussa aiheessa pysyttiin ja tutkimuksen lopputuloksena syntynyt malli on hyödyllinen hotellialan toimijoille.

Kyberuhkien tuntemisen tärkeys tiedostetaan hotellialalla, mutta nykyisellään siihen ei puututa tarpeeksi, eikä henkilöstöä kyberkouluteta asianmukaisesti. Tämän opinnäytetyön ja Kyberuhkien Kartoituksen Kidemallin avulla on mahdollista tunnistaa kohdehotellin kyberuhat ja sen perusteella voidaan toteuttaa uhka-analyysi. Opinnäytetyön tekijöiden mielestä opinnäytetyössä esitetyt uhat ovat sellaisia uhkia, joihin olisi hyvä varautua lähitulevaisuudessa. Työssä keskitytään lähitulevaisuuteen, minkä takia siinä esitetyt muutokset ja uhat ovat tietyltä osin vain ennustamista. Aloittaessaan opinnäytetyöprosessia opinnäytetyöntekijöillä oli tiedossa työn ennusteenomainen luonne. Tästä huolimatta opinnäytetyön aihe koettiin hyödylliseksi ja tarpeelliseksi, sillä kyberuhkia ei ole käsitelty Suomessa hotellialan näkökulmasta juuri yhtään.

Tietoperustan kokoaminen aloitettiin etsimällä relevantteja kirja- ja verkkolähteitä. Etenkin verkkolähteitä käytettäessä pyrittiin tarkastelemaan kriittisesti niiden luotettavuutta. Kirjallisuuslähteissä käytettiin aina tuoreinta saatavilla olevaa materiaalia. Suurin osa verkkolähteistä on enintään muutaman vuoden vanhoja, millä haluttiin varmistaa ajankohtaisimman tiedon saaminen. Tietoperustan kasaamiseen haasteita toi aiheen vähäinen käsittely kotimaisessa kirjallisuudessa tai verkkolähteissä, etenkin hotellialan näkökulmasta. Edellä mainitusta syystä opinnäytetyössä on käytetty paljon kansainvälisiä verkkolähteitä. Kansainvälisten lähteiden kääntäminen suomenkielelle oli ajoittain haastavaa, sillä virallisia käännöksiä kaikille kyberturvallisuutta koskeville termeille ei ole. Erityisen mielenkiintoista tietoperustan luomisessa opinnäytetyön tekijöille oli case-esimerkkien kerääminen, sillä niistä parhaiten tajuaa aiheen moninaisuuden. Case-esimerkit olivat myös todella opettavaisia ja auttoivat ymmärtämään kokonaisuutta. Tietoperustasta tuli opinnäytetyön tekijöiden näkökulmasta tiedollisesti riittävän laaja perustelemaan käytännön tutkimusta. Tietoperustaa tukemaan kirjoitettiin termistö, jonka tarkoituksena on auttaa lukijaa ymmärtämään opinnäytetyössä käytettyjä termejä. Laajaa tietoperustaa voitiin verrata haastatteluihin hyvin ja sen avulla onnistuttiin luomaan eheä kokonaisuus.

Opinnäytetyön tekeminen aikataulutettiin ennen kirjoittamisen aloittamista. Tietoperusta suunniteltiin toteutettavan viikkojen 37 ja 42 välisenä aikana. Tässä tavoitteessa pysyttiin erinomaisesti. Haastattelut suunniteltiin toteutettavan viikkojen 38 ja 40 välisenä aikana, mutta haastateltavan muuttuneiden aikataulujen takia viimeinen haastattelu toteutettiin vasta viikolla 44. Asiantuntijahaastatteluita sovittiin suunnitellusti viisi, mutta yksi peruuntui ja tiukan aikataulun vuoksi sitä ei saatu enää järjestymään. Muutoksiin oli kuitenkin varauduttu, eivätkä ne näkyneet lopullisen aikataulun venymisenä. Lopulta haastatteluja suoritettiin neljä, joista saatiin tarpeeksi monipuolisesti vastauksia tutkimuskysymyksiin. Yhtä haastattelua lukuun ottamatta opinnäytetyö toteutettiin suunnitellusti ja opinnäytetyö valmistui aikataulussa. Aikataulussa pysyttiin näin onnistuneesti, sillä opinnäytetyön tekijöillä oli käytössä yhteinen kalenteri ja opinnäytetyön tekemiselle oli alusta asti varattu paljon aikaa. Opinnäytetyön tekemisen tavoitteet oli asetettu korkealle ja molemmilla työn tekijöillä oli motivaatiota täyttää ne.

Kvalitatiivisessa tutkimuksessa haastattelujen määrä olisi voinut olla suurempi, jolloin haastattelujen tulokset olisivat olleet entistä luotettavammat. Kyberturvallisuuden ollessa aiheena arkaluontoinen oli haastateltavien kokoaminen haastavaa. Lopulta haastateltavat saatiin kasattua opinnäytetyön tekijöiden omista verkostoista ja lupaamalla haastateltaville anonymiteetti. Haastattelupyyntöjä lähetettiin usealle eri taholle, mutta moniin ei saatu ollenkaan vastausta. Opinnäytetyöhön valikoituneet haastateltavat oli suunniteltu olevan mukana alun perinkin, mutta mahdollisia muutostilanteita varten haastateltavia haluttiin pyytää useampi.

Tutkimuksen onnitumista pohdittaessa on otettava ensin huomioon, onko tutkimusmenetelmän valinta ollut onnistunut. Kvalitatiivisen tutkimusmenetelmän valinta ja päätös toteuttaa se teemahaastatteluina oli opinnäytetyön tekijöiden mielestä oikea valinta. Täysin strukturoidulla haastattelulla ei olisi saatu tarkoituksenmukaisia vastauksia. Luomalla yksilöidyt haastattelukysymykset yhtenevin teemoin saatiin kattavammat vastaukset tutkimuskysymyksiin. Tutkimuksen tekeminen oli opinnäytetyön tekijöille mieluisaa ja palkitsevaa. Erityisesti haastattelut toivat paljon uusia näkökulmia aiheeseen. Haastattelujen määrä koettiin riittäväksi, sillä haastatteluissa tuli esille paljon keskenään yhteneväisiä vastauksia. Tästä johtuen useamman haastattelun määrä ei välttämättä olisi tuonut enää lisäarvoa tutkimukselle. Vastaukset olivat linjassa myös tietoperustan kanssa, jonka vuoksi niitä voidaan pitää luotettavina. Täysin varmaa tietoa opinnäytetyön tutkimuksella ei voitu saavuttaa, sillä tulevan ennustamiseen liittyy aina tietty virhemarginaali.

Tutkimuksen tuloksena saatiin kuusi hotellialan lähitulevaisuuden muutosta ja niihin liittyvät kymmenen todennäköisintä kyberuhkaa. Tuloksista luotiin Kyberuhkien Kartoittamisen Kidemalli sekä sen selvitysosa helpottamaan mallin lukemista. Opinnäytetyön tulosten perusteella mallin tekeminen päätettiin jo tutkimusta suunniteltaessa, mutta mallin luonne muovautui vasta tuloksia arvioitaessa. Mallin luominen oli mielekästä sekä innovatiivista. Mallin luominen ja suunnittelu toivat vaihtelua kirjoittamiseen. Opinnäytetyön tekijät kokevat mallin tuovan lisäarvoa hotellialan toimijoille ja toivovat, että sitä hyödynnetään jo muutoksia suunniteltaessa. Jatkoa ajatellen olisi hyvä tehdä tutkimuksia kyberuhkien toistuvuuksista sekä niiden taloudellisista vaikutuksista Suomessa, näin malli toisi entistä tarkempaa tietoa. Malli toimii sellaisenaan, kunnes siinä mainitut muutokset on otettu laajasti käyttöön, jonka jälkeen se voidaan päivittää.

8.1 Jatkotutkimusaiheet

Opinnäytetyötä ja rajausta suunniteltaessa jäi työn ulkopuolelle monia kiinnostavia kokonaisuuksia, kuten miten lähitulevaisuuden kyberuhkiin tulisi varautua? Mitä tahattomia kyberuhkia hotelliala voi kohdata? Miten henkilöstöä tulisi kyberkouluttaa? Nämä ovat opinnäytetyön tekijöiden mielestä erittäin mielenkiintoisia aiheita ja niiden toteuttaminen opinnäytetyönä olisi ollut yhtä mielenkiintoista, kuin valittu aihe. Kuitenkin hotellialan tulevien kyberuhkien tutkiminen on välttämätöntä ennen kuin voidaan tutkia miten niihin tulisi varautua. Jotta voidaan tutkia, miten henkilöstöä tulisi kyberkouluttaa täytyy myös tutkia, mitä vastaan henkilöstö tulisi kouluttaa. Tahattomien kyberuhkien tutkimisen sisällyttäminen olisi taas tehnyt työstä liian laajan. Opinnäytetyön tekijöiden mielestä kaikki kolmesta mainitusta jatkotutkimusaiheesta kelpaisi tutkimuksen aiheeksi sellaisenaan.

8.2 Prosessin ja oman oppimisen arviointi

Opinnäytetyön toteutus sujui suunnitellusti ja hyvin. Opinnäytetyön aihe oli opinnäytetyön tekijöillä valittuna jo ennen prosessin aloitusta. Opinnäytetyön tekijät olivat työskennelleet useissa opintoihin liittyvissä projekteissa yhdessä, jonka vuoksi tiedettiin, että parityöskentely tulee sujumaan. Aiemman kokemuksen ja yhteisen kiinnostuksen perusteella päätettiin opinnäytetyö toteuttaa parityönä. Työ päätettiin toteuttaa parityönä myös sen vuoksi, että aihetta olisi mahdollista tutkia laajemmin, kuin mitä yksilötyönä tehdyssä opinnäytetyössä olisi ollut mahdollista. Alusta asti aikataulutuksen tärkeys oli tekijöillä tiedossa. Prosessia aloittaessa otettiin käyttöön yhteinen kalenterisovellus, johon määritettiin kaikki prosessiin liittyvät tapaamiset, omat määräajat ja palautuspäivät. Kalenterin käyttöönotto oli erinomainen päätös ja se teki projektin hallinnasta sujuvaa.

Työ toteutettiin täysin yhteistyönä, sillä opinnäytetyön tekijät eivät kirjoittaneet työtä erikseen. Tähän ratkaisuun päädyttiin, jotta teksti olisi yhtenäistä läpi työn ja laatu tasaista. Yhteiselle kirjoittamiselle perusteena oli myös se, että molemmat opinnäytetyön tekijät tuntisivat työn kaikki osa-alueet yhtä kattavasti.

Opinnäytetyön rajaus pyrittiin alusta asti tekemään tarvittavan tiukasti. Opinnäytetyön tekijöillä oli tiedossa, että ilman tiukkaa rajausta työhön olisi tullut helposti tavoitteen kannalta turhaa tietoa. Opinnäytetyön tavoitteet pidettiin mielessä koko prosessin ajan ja jokaisella aiheella pyrittiin vastaamaan johonkin työn tutkimuskysymyksistä. Tämän vuoksi opinnäytetyön kirjoittaminen oli mielekästä, eikä työstä tarvinnut rajata ulos sen kirjoittamisen jälkeen juuri mitään.

Opinnäytetyön aiheesta hotelliala oli työn tekijöille entuudestaan tuttu opintojen kautta, kun taas kybertoimintaympäristö aiheena oli tekijöille lähes tuntematon. Aihetta valittaessa tiedostettiin tämän tuomat haasteet, mutta halu oppia aiheesta oli suuri. Kybertoimintaympäristöstä kirjoittaminen ja aiheen tutkiminen olivat haastavaa, mutta erittäin antoisaa. Opinnäytetyön tekeminen laajensi myös hotellialan tuntemusta ja toi aivan uusia näkökulmia alan kehityksestä. Opinnäytetyön tekijät kokevat hotellialan kybertietoisuuden olevan tärkeää ja hyödyllistä ammatillista kehitystä ja tulevaisuutta ajatellen.

Lopuksi; aiheen valinta oli erittäin onnistunut, työtä oli ilo tehdä ja tutkimustulokset olivat tavoitteiden mukaiset.

Lähteet

Accenture 2017. 2017 Cost of Cyber Crime Study. Luettavissa: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf. Luettu: 25.9.2018.

Ajmera A. 2017. Reuters. Hyatt Hotels discovers card data breach at 41 properties. Luettavsissa: https://www.reuters.com/article/us-hyatt-hotels-cyber/hyatt-hotels-discovers-card-data-breach-at-41-properties-idUSKBN1CH2WP. Luettu 15.10.2018.

Autio A. 2017. Keskisuomalainen. Ulkomaiset hotelliketjut laajentavat Suomessa – lisää voi olla tulossa. Luettavissa: https://www.ksml.fi/talous/Ulkomaiset-hotelliketjut-laajentavat-Suomessa%E2%80%89–%E2%80%89lisää-voi-olla-tulossa/1072201. Luettu 8.10.2018.

Bhattarai A. 2017. The Washington Post. Hackers have been stealing credit card numbers from Trump's hotels for months. Luettavissa: https://www.washingtonpost.com/news/business/wp/2017/07/11/hackers-have-been-stealing-credit-card-numbers-from-trumps-hotels-for-months/?noredirect=on&utm_term=.c698203a1205. Luettu: 10.10.2018.

Bilefsky D. 2017. The New York Post. Hackers Use New Tactic at Austrian Hotel: Locking the Doors. Luettavissa: https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html. Luettu: 10.10.2018.

Biswas & Santhana 2017. Deloitte. Blockchain risk management. Luettavissa: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-blockchain-risk-management.pdf. Luettu: 10.11.2018.

Bradford L. 2018. Forbes. What You Need To Know About Cybersecurity In 2018. Luettavissa: https://www.forbes.com/sites/laurencebradford/2018/03/30/why-people-should-learn-about-cybersecurity-in-2018/#4a70225b5d00. Luettu: 1.10.2018.

citizenM. A new breed of hotel. Luettavissa: https://www.citizenm.com/global/company. Luettu: 16.10.2018.

Davis, K. 2018. The 3 Most Frequent Cybersecurity Threats Against Hotels. Kevin Davis Insurance Services. Luettavissa: https://www.kdisonline.com/3-most-frequent-cybersecurity-threats-against-hotels/. Luettu 29.9.2018.

DigFin 2018. MasterCard pushes biometric in Asia. Luettavissa: https://www.digfingroup.com/mastercard/. Luettu: 10.11.2018.

Disparte, D. & Furlow, C. 2017. Harward Business Review. The best cybersecurity investment you can make is better training. Luettavissa: https://hbr.org/2017/05/the-bestcybersecurity-investment-you-can-make-is-bettertraining?referral=03759&cm_vc=rr_item_page.bottom. Luettu: 1.10.2018.

Dogru, T., Mody M. & Leonardi C. 2018. Blockchain Technology & its Implications for the Hospitality Industry. Luettavissa: file:///C:/Users/User/Downloads/Blockchain-Technology-and-its-Implications-for-the-Hospitality-Industry.pdf. Luettu: 30.10.2018.

ENISA European Union Agency for Network and Information Security 2017. Top 15 cyber threaths in 2017. Luettavissa: https://etl.enisa.europa.eu/#/. Luettu 18.9.2018.

Eur-Lex 2013. Komission asetus (EU) N:o 611/2013. Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32013R0611. Luettu: 6.11.2018.

Gopalakrishnan R. & Mogato M. 2016. Reuters. Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. Luettavissa: https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH. Luettu: 28.11.2018.

Henn Na Hotel. Henn na Hotel General Concept. Luettavissa: http://www.h-n-h.jp/en/concept/. Luettu: 16.10.2018.

Hiisi Homes & Hotels 2018. Open the door for the future with a mobile key. Youtube video. Hiisi Homes & Hotels kanava. Nähtävissä: https://www.youtube.com/watch?v=_utyDq4bYbE. Nähty: 5.11.2018.

Hiltunen, E. 2017. Mitä tulevaisuuden asiakas haluaa. Trendit ja ilmiöt. Docendo Oy. Jyväskylä.

Hirsjärvi & Hurme 2011. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Gaudeamus Helsinki University Press Oy Yliopistokustannus. Tallinna.

Hospitality & Catering News 2012. Enhanced guest experience at new London citizenM. Luettavissa: https://www.hospitalityandcateringnews.com/2012/07/enhanced-guest-experience-at-new-london-citizenm/. Luettu: 16.10.2018.

Hyatt 2016. Hyatt Completes Payment Card Incident Investigation. Luettavissa: https://newsroom.hyatt.com/news-releases?item=123453. Luettu: 15.10.2018

Hämäläinen K. 2018. Taloustaito. Hotellin omistajaksi huone kerrallaan – 14 prosentin tuotolla? Luettavissa: https://www.taloustaito.fi/Rahat/hotellin-omistajaksi-huone-kerrallaan--14-prosentin-tuotolla/. Luettu: 28.11.2018.

Jaremen D., Jędrasiak M. & Rapacz A. 2016. The Concept of Smart Hotels as an Innovation on the Hospitality Industry Market – Case Study of Puro Hotel in Wrocław. Luettavissa: file:///C:/Users/User/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/The_Concept_of_Smart_Hotels_as_an_Innovation_on_th%20(1).pdf. Luettu: 10.10.2018.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Docendo Oy. Jyväskylä.

If 2018. Kyberterminologiaa. Luettavissa: https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/kyberterminologiaa.Luettu: 18.9.2018.

If 2017. Tavanomaisia sanoja ja ilmaisuja kybermaailmassa. Luettavissa: https://www.if.fi/globalassets/fi/commercial/brochures/vastuuvakuutus/66752-kybersanasto.pdf. Luettu: 18.9.2018.

Kaur T. 2017. Forbes. On The Edge: Five High-Tech Hotels In Asia For Tech-Savvy Travelers. Luettavissa: https://www.forbes.com/sites/tarandipkaur/2017/11/14/on-the-edge-five-high-tech-hotels-in-asia-for-tech-savvy-travelers/#23de7c5b7f84. Luettu: 11.10.2018.

Kobres E. 2018. Forbes. New Technologies Will Revolutionize The Hospitality Industry. Luettavissa: https://www.forbes.com/sites/forbestechcouncil/2018/06/28/new-technologies-will-revolutionize-the-hospitality-industry/#1839ede873c3. Luettu: 11.10.2018.

KrebsonSecurity 2016. Hyatt Card Breach Hit 250 Hotels in 50 Nations. Luettavissa: https://krebsonsecurity.com/2016/01/hyatt-card-breach-hit-250-hotels-in-50-nations/. Luettu: 15.10.2018.

Kryptot.net. Mitä ovat kryptovaluutat?. Luettavissa: https://kryptot.net/. Luettu: 16.10.2018.

Le Gall B. 2017. Hoist Group AB Oy. Mobiiliavain. Luettavissa: https://www.hoistgroup.com/fi/uutiset-lehdisto/2017/07/04/mobiiliavain/. Luettu: 5.11.2018.

Limnell, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Docendo Oy. Jyväskylä.

Norton. Malware 101: What is a botnet? Luettavsissa: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html. Luettu: 25.10.2018.

Oberhaus D. 2017. Motherboard. This Luxury Hotel Is Sick of Ransomware Attacks, So It's Going Analog. Luettavissa: https://motherboard.vice.com/en_us/article/nzdznb/luxury-hotel-goes-analog-to-fight-ransomware-attacks. Luettu: 10.10.2018.

Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon: näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum. Helsinki.

Quadir S. 2016. Reuters. How a hacker's typo helped stop a billion dollar bank heist. Luettavissa: https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight/how-a-hackers-typo-helped-stop-a-billion-dollar-bank-heist-idUSKCN0WC0TC. Luettu: 24.10.2018.

Radisson Blu 2018. One Touch-sovellus. Luettavissa: https://www.radissonblu.com/fi/tietoja-yrityksesta#/one-touch-app. Luettu: 10.10.2018.

Raeste J-P. 2018. Helsingin Sanomat. Helsinkiin on syntymässä toistakymmentä uutta hotellia – silti Suomessa ollaan vielä jäljessä muita Pohjoismaita. Luettavissa: https://www.hs.fi/talous/art-2000005584807.html. Luettu: 8.10.2018.

Rautiainen, M. & Siiskonen M. 2015. Majoitustoiminta ja palveluosaaminen. Restamark Oy. Vantaa.

Refine. Blockchain Technology and Its Uses in the Hospitality Industry. Luettavissa: https://www.revfine.com/blockchain-technology-hospitality-industry/. Luettu: 25.10.2018.

Rissanen V. 2018. Helsingin Sanomat. Suomalainen työpari keksi keinon, jolla voi luoda yleisavaimen hotelleihin ympäri maailman – Katso HS:n videolta, miten laite toimii. Luettavissa: https://www.hs.fi/teknologia/art-2000005655928.html. Luettu: 16.10.2018.

Roberts, P. 2018. Digital Guardian. Hilton Was Fined $700K for a Data Breach. Under GDPR It Would Be $420M. Luettavissa: https://digitalguardian.com/blog/hilton-was-fined-700k-data-breach-under-gdpr-it-would-be-420m. Luettu: 10.10.2018.

Sabre 2017. Sabre Update on Cybersecurity Incident. Luettavissa: https://www.sabre.com/insights/releases/sabre-update-on-cybersecurity-incident/.

Sanastokeskus TSK ry 2018. Kyberturvallisuuden sanasto. Huoltovarmuuskeskus. Helsinki. Luettavissa: http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf. Luettu: 31.10.2018.

Scandic Hotels. Yli 5000 lehteä maksutta. Luettavissa: https://www.scandichotels.fi/aina-scandicissa/pressreader. Luettu. 10.10.2018.

Shabani, N. 2016. A study of cyber security in hospitality industry – threats and countermeasures: case study in Reno Nevada. Luettavissa: https://arxiv.org/pdf/1705.02749.pdf. Luettu: 23.9.2018.

Skift 2018. Megatrends defining travel in 2018. Luettavissa: https://skift.com/wp-content/themes/skift/img/megatrends-2018//Skift-Megatrends-2018.pdf. Luettu: 11.10.2018.

Stempel J. 2017. Reuters. Hilton to pay $700,000 over credit card data breaches. Luettavissa: https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3. Luettu: 10.10.2018.

SSA Base 2018. Näin se toimii. Luettavissa: https://basemansku.fi/nain-base-toimii/. Luettu: 10.10.2018.

The Trump Hotels 2017. Notice regarding guest payment card information. Luettavissa: https://www.trumphotels.com/uploads/14111/0/trump-sabre-notice-website-letter.pdf. Luettu: 10.10.2018.

Tilastokeskus 2018a. Käsitteet ja määritelmät. Luettavissa: https://www.stat.fi/til/matk/kas.html. Luettu: 10.10.2018.

Tilastokeskus 2018b. Majoituspalveluiden kysyntä nousi ennätyslukemiin 2017. Luettavissa: http://tilastokeskus.fi/til/matk/2017/matk_2017_2018-04-19_tie_001_fi.html?ad=notify. Luettu: 3.10.2018.

Ting D. 2017. Skift. Hilton Must Pay $700,000 for Two of Its Credit Card Data Breaches. Luettavissa: https://skift.com/2017/11/02/hilton-must-pay-700000-for-two-of-its-credit-card-data-breaches/. Luettu: 10.10.2018.

TrendWatching 2017. The Bigger Picture. Luettavissa: https://trendwatching.com/quarterly/2017-03/the-bigger-picture/. Luettu: 11.10.2018.

Ulkoministeriö. Luettavissa: https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto. Luettu: 18.9.2018.

Vainio J. 2016a. Kaleva. Analyysi: Harkitse vakavasti Hotels.com-sivuston käyttöä – sivustosta satelee rikosilmoituksia. Luettavissa: https://www.kaleva.fi/uutiset/kotimaa/analyysi-harkitse-vakavasti-hotelscom-sivuston-kayttoa-sivustosta-satelee-rikosilmoituksia/731891/. Luettu: 15.10.2018.

Vainio J. 2016b. Turun Sanomat. Rahat lähtevät tileiltä – poliisille satoja ilmoituksia sivustosta. Luettavissa: https://www.ts.fi/uutiset/kotimaa/862300/Rahat+lahtevat+tileilta++poliisille+satoja+ilmoituksia+sivustosta. Luettu: 15.10.2018.

Viljanen M. 2017. Kauppalehti. Hotelliala kasvaa Suomessa muita Pohjoismaita nopeammin. Luettavissa: https://www.kauppalehti.fi/uutiset/hotelliala-kasvaa-suomessa-muita-pohjoismaita-nopeammin/Lrpy9UeD. Luettu: 3.10.2018.

Liitteet

Liite 1. Haastattelukysymykset, haastateltava 1.

Nykytila

- Kerro lyhyesti, miten olet päätynyt nykyiseen virkaasi?
- Millaista teknologiaa on jo käytössä Suomen hotellialalla, joka on edistyksellistä esim. lukot?
- Mitä hotellivarausjärjestelmiä tällä hetkellä on käytössä suomen markkinoilla?
- Mihin suuntaan näet hotellivarausjärjestelmien liikkuvan?

Tulevaisuus

- Oma suosikkitrendisi, jonka toivot leviävän hotellialalle?
- Mitkä ovat mielestäsi isoimmat muutokset hotellialalla?
- Kuinka teknologia tulee muuttamaan hotellialaa?
- Millaista teknologiaa uskot tulevan hotellialalle lähitulevaisuudessa?
- Miten rahan käyttö hotelleissa tulee muuttumaan (mikrosirut, mobilepay, elektroninen henkilökortti jne.)
- Tuleeko Smart-hotellista oma konseptinsa vai tuleeko kaikista hotelleista Smart-hotelleja?

Turvallisuus

- Onko hotelliala Suomessa kohdannut kyberturvallisuuteen liittyviä uhkia?
- Millainen on mielestäsi kyberuhkiin varautumisen tila hotellialalla Suomessa?
- Kuinka laaja ongelma kyberuhat ovat hotellialalla?
- Mitkä tulevat olemaan tulevaisuuden kyberuhkia?
- Miten näihin tulevaisuuden uhkiin voisi varautua?

Liite 2. Haastattelukysymykset, haastateltava 2.

Tausta

- Minkä tyyppisessä yrityksessä olet töissä (esim. suuri/kotimainen/ala)
- Mikä on asemasi yrityksessä? (johtoporras, toimihenkilö tms.)

Kyberhyökkäykset

- Minkälaisia kyberturvallisuuteen liittyviä uhkia olette kohdanneet edellisen viiden vuoden aikana?
- Millaisia vaikutuksia hyökkäyksillä oli?
- Kuinka paljon työtunteja meni hukkaan?
- Minkälaisia taloudellisia vaikutuksia hyökkäyksillä oli?
- Aiheuttiko hyökkäys luottamuspulaa asiakkailta, mikäli hyökkäykset tulivat asiakkaiden tietoon?
- Onko hyökkäysten tekotapa saatu selville ja minkä heikkouden kautta hyökkäys tapahtui?
- Jos työntekijät olisivat tietoisempia ja koulutetumpia kyberriskejä vastaan, olisiko hyökkäykset ollut mahdollista torjua?

Kyberhyökkäysten jälkeen

- Millaisten toimien uskot ehkäisevän kyberuhkia?
- Mitä olette oppineet yrityksenä hyökkäyksistä?
- Kokemuksen perusteella, mitä nyt tekisitte toisin, jos kokemattomana yrityksenä varautuisitte kyberuhkiin?
- Onko edellisten kyberhyökkäysten jälkeen tehtyjen toimien perusteella pystytty tiedettävästi ehkäisemään uusia hyökkäyksiä?

Liite 3. Haastattelukysymykset, haastateltava 3.

Now

- We know you have a lot of specialty's but tell us shortly how you started working with hotels and concept development?
- What is your opinion of hotel industry in Finland?
- Do you think it is lacking behind with trends compared to Nordic countries, Netherlands, Germany and other European countries?

Future

- What's your favourite current trend and what are the upcoming trends that you are most exited about?
- How do you see hotel industry will change in the near future?
- In terms of technology, what is the future of hotels?
- In your opinion how will technology change hotels in the future?
- Do you think there will be new methods of payment (for example microchips)?
- Will Smart-hotels stay as their own concept or will all hotels become Smart-hotels?
- Do you think smart and individualised rooms will become norm in the future? (like the ability to control the lights and air-conditioning with their mobile phone)
- What do you think is the best balance of technology and humanity in hospitality industry?

Safety

- Do you think hotel industry is becoming more fragile or more resilient due technology?

Liite 4. Haastattelukysymykset, haastateltava 4.

Tausta

- Kerro vähän itsestäsi?
- Tausta hakkeroinnissa?
- Minkälaisena hakkerina pidät itseäsi?
- Mikä sinua motivoi?

Nykytila

- Hakkerointi nykypäivänä keskittyy luottokorttitietoihin ja muihin henkilötietoihin, mihin muuhun hakkeroinnilla voidaan iskeä hotellissa
- Mihin se voi tulevaisuudessa kohdistua?
- Mitä virheitä ihmiset tekevät eniten?
- Mitkä tällä hetkellä ovat suurimmat riskit?
- Mitä muuta kuin rahallista vahinkoa voidaan hotelleille tehdä?

Tulevaisuus

- Kun hotelleissa lisääntyy älypuhelinten/muiden laitteiden kautta tehtävät säädöt (esim. lämmitys. Ilmastointi, valot), jota käytetään hotellin verkossa, miten tämän järjestelmän kautta voisi aiheuttaa haittaa hotellille ja/tai asiakkaiden tiedoille?
- Mitkä ovat mielestäsi biometrisen tunnistuksen riskit?
- Mikäli hotellit siirtyisivät käyttämään blockchainia, niin mitä riskejä se toisi tullessaan vai olisiko se turvallisempaa?
- Mihin hotellien kannattaisi alkaa panostaa jo nyt, joka hyödyttäisi tulevaisuudessa?
- Mihin uskot hakkeroinnin tulevaisuudessa kohdistuvan enenemissä määrin?
- Miten hotellit voisivat hyötyä hakkereista?

Liite 5. Lupa TrendWatching kuvan käyttöön

Mega-trends image usage

PB **Paul Backman <paul@trendwatching.com>**
6.11.2018 18.08

Vastaanottaja: elli.ojankoski@live.com

Hi Elli,

Thank you for getting in touch.

You're free to use our mega-trends image in your thesis for non-commercial usage as long as TrendWatching (www.trendwatching.com) is credited as the source.

All the very best

Paul

Paul Backman
Global Futures Director

TrendWatching
paul@trendwatching.com
+44 20 7251 6811
+44 7811 401 356
WhatsApp