Yrityksen kyberturvallisuuden nykytila-analyysi

Samuel Laitinen

2023 Laurea Leppävaara

Laurea-ammattikorkeakoulu

Yrityksen kyberturvallisuuden nykytila-analyysi

Samuel Laitinen

Tietojenkäsittely

Opinnäytetyö

11,2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Liiketalouden ammattikorkeakoulututkinto

Tietojenkäsittely (AMK)

Samuel Laitinen

Yrityksen kyberturvallisuuden nykytila-analyysi

Vuosi 2023 Sivumäärä 45

Tämä opinnäytetyö toteutettiin toimeksiantajalle matkailu- ravintola- ja tapahtuma-alan yritykselle heidän tarpeestaan kehittää kyberturvallisuuttaan, jota aiemmin ei oltu juurikaan huomioitu. Opinnäytetyön tarkoituksena oli selvittää kohdeyrityksen kyberturvallisuuden nykytila sekä siihen vaikuttavat tekijät, ja antaa ohjeistuksia kyberturvallisuuden kehittämiseksi ja ylläpitämiseksi. Tavoitteena oli, että tekemäni nykytila-analyysin pohjalta yritys tiedostaa lähtökohdat, jonka jälkeen se voi laittaa kyberturvallisuuden perustason toimenpiteet kuntoon ja valjastaa kyberturvallisuuden osaksi yrityksen arkea. Opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä ja menetelminä käytettiin sekä laadullisia että määrällisiä tutkimusmenetelmiä. Opinnäytetyön kokonaisuus koostui teoriakatsauksesta, yritysjohdon teemahaastattelusta, Kyberturvallisuuskeskuksen kybermittari- työkalun testeistä, tulosten analyysista SWOT-nelikenttämallin avulla sekä kehitysehdotusten ja jatkotoimenpiteiden esittämisestä.

Tulosten perusteella yrityksen kyberturvallisuuden nykytila on kohtalainen. Yrityksessä ei oltu juurikaan ennen kiinnitetty huomiota kybertuvallisuuteen. Yrityksessä hoidetaan kuitenkin esimerkiksi tärkeiden tietojen asianmukainen suojaus, palomuurit, virustorjunta, verkkojen suojaukset sekä käyttöoikeudet lähtökohtaisesti hyvin. Suurimpia puutteita taas oli yleisten toimintatapojen, suunnitelmien, seurannan ja raportoinnin puuttuminen. Yrityksen vahvuuksina nousi esiin yrityksen hallinnollisesti hyvät valmiudet parantaa kyberturvallisuuden nykytilaa ja tarvittavien resurssien ja osaamisen olemassaolo. Mahdollisuutena nähtiin kyberturvallisuuden kehittäminen yhteistyössä olemassa olevan hyvän IT-alan kumppanin kanssa. Heikkoutena kuitenkin on, ettei kyberturvallisuuden merkitystä olla tunnistettu eikä suurta uhkaa koeta olevan. Myös henkilökunnan tietoturvaosaaminen on heikkoa. Uhkana havaittiin, ettei ulkopuolisia uhkia tunnisteta eikä kybertoimintaympäristöä hahmoteta. Jatkotoimenpiteinä ehdotetaan tiiviimpää yhteistyötä IT-alan kumppanien kanssa ja kyberturvallisuussuunnitelman laatimista heidän kanssaan yhdessä.

Asiasanat: kyberturvallisuus, kyberuhka, kyberriskienhallinta, nykytila-analyysi

Laurea University of Applied Sciences **Abstract**

Business Information Technology

Bachelor of Business Administration (BBA)

Samuel Laitinen

An analysis of the current state of cybersecurity at a case company

Year 2023 Pages 45

This project was carried out for the client, a company in the tourism, restaurant and event management sector. The purpose of the thesis was to determine the current status of the target company's cyber security and the factors that affect it, and to provide guidelines for developing and maintaining their cyber security. The thesis was carried out as a research development work and the author used both qualitative and quantitative methods. The entirety of the thesis consisted of a theory review, a themed interview of the company management, tests of the Cybersecurity Center's cyber meter tool, analysis of the results using the SWOT four-field model, and presentation of development proposals and further measures.

Based on the results, the current state of the company's cyber security is moderate. The company had not paid much attention to cyber security before. However, the company has handled, for example the appropriate protection of important data, firewalls, virus protection, network protections and user rights basically well. The biggest shortcomings were the absence of general operating procedures, plans, monitoring and reporting. The company's good administrative capabilities to improve the current state of cyber security and the existence of the necessary resources and expertise emerged as the biggest strengths. Developing cyber security in cooperation with an existing good partner in the IT industry was seen as a possibility. However, the weakness is that the importance of cyber security has not been recognized and there is no perceived threat. The information security skills of the staff are also weak. The threat was found to be that external threats are not recognized and the cyber environment is not understood. Closer cooperation with the partners in the IT sector and the preparation of a cyber security plan together are proposed as follow-up measures.

Keywords: cyber security, cyber threat, cyber risk management, current state analysis

Sisällys

1 Johdanto

Maailma ja yhteiskunta digitalisoituu kovaa vauhtia, mikä tuo suurten liiketoimintahyötyjen lisäksi myös uudenlaisia haasteita. Kyberuhat ovat huomattavasti lisääntyneet viime aikoina, kuten myös niiden haitalliset vaikutukset. Kyberturvallisuus on trendikäs aihe nykymaailmassa ja kyberrikolliset etsivät koko ajan uusia keinoja päästä turvatoimien läpi ja päästä varastamaan luottamuksellisia tietoja. Aihetta nostaa pinnalle entisestään Venäjän hyökkäys Ukrainaan helmikuussa 2022, joka toi esiin kybersodankäynnin ja kybervaikuttamisen eri muotoja. Muutokset kansainvälisessä turvallisuustilanteessa korostavat myös yritysten varautumisen tärkeyttä. Myös koronaviruspandemia toi uusia haasteita ja uusia väyliä kyberrikollisille toimia kun 2020 työntekijät siirtyivät nopeasti etätöihin kotitoimistoille eikä tietoturvaa näissä ratkaisussa aina huomioitu.

Monissa yrityksissä puuttuu vielä kokonaan osaaminen kyberturvallisuudesta eikä kyberuhkiin olla osattu varautua oikein. Tässä työssä haluan tuoda esiin, kuinka jokaisen organisaation, niin pienten kuin suurien ja kaikilta aloilta, tulisi suojella itseään kyberuhilta sekä rakentaa ja kehittää jatkuvasti kyberturvallisuuttaan, viimeistään nyt. Monilta kyberuhkilta on kuitenkin mahdollista suojautua laittamalla ihan vain perusasiat kuntoon. Tämä tutkimuksellinen kehittämistyö kohdistuu pieneen yritykseen, jossa kyberturvallisuutta ei olla juurikaan vielä huomioitu, vaikka siihen on viime aikoina kohdistunut paljon erilaisia tietojenkalastelu- ja huijausyrityksiä.

Tarkoituksena on selvittää toimeksiantajayrityksen kanssa heidän kyberturvallisuuden lähtötaso ja siihen vaikuttavat tekijät, ja näiden pohjalta antaa muutamia kehitysideoita, kuinka kyberturvallisuuden parantamisessa voitaisiin yrityksessä edetä yrityksen tarpeet ja koko huomioiden. Opinnäytetyön tarkoituksena on tehdä kattava nykytila-analyysi yrityksen hyödyksi, jonka avulla he voivat lähteä parantamaan kyberturvallisuuttaan kun lähtötaso on ensiksi selvillä. Tavoitteena on, että nykytila-analyysin pohjalta yritys pääsisi rakentamaan toimivaa kyberturvallisuusympäristöä sekä löytää työkaluja ja toimenpiteitä kyberturvallisuuden edistämiseen, jotta saavat laitettua ns. perusasiat kuntoon. Tavoitteena on auttaa kohdeyritystä ottamaan kyberturvallisuuden osaksi heidän arkeaan ja auttaa ymmärtämään suojautumisen tärkeyden. Tutkimuksellisen kehittämishankkeen kohdistuessa pieneen, yhteiskunnan kannalta ei niin kriittisiä toimintoja omaavaan yritykseen, tulee kiinnittää huomiota siihen, ettei kyberturvallisuuteen saa kuitenkaan laittaa resursseja liikaa, ettei se vie huomiota pois muusta tärkeästä toiminnasta. Tärkeää on löytää tässä sopiva tasapaino.

Tutkimuksellisen kehitystyön tutkimusmetodiksi valikoitui tapaustutkimus eli case-tutkimus kohdeyritykseen. Tutkimuksen aineisto koostuu kohdeyrityksen omistajien haastattelusta,

laajasta teoriakatsauksesta sekä Kyberturvallisuuskeskuksen kybermittari – työkalun tuloksista. Lopuksi vielä kasaan saadut tulokset SWOT-nelikenttämalliin ja esitän kehitysehdotuksia ja jatkotoimenpiteitä kyberturvallisuuden parantamiseksi. Opinnäytetyön ensimmäinen luku johdannon jälkeen johdattaa tutkimuksellisen kehitystyön aiheeseen sekä asettaa työn tavoitteet. Ensimmäisessä teorialuvussa 3 määritellään kyberturvallisuuden ja työn kannalta merkityksellisimpiä käsitteitä, jonka jälkeen luvussa 4 syvennytään näihin lisää avaamalla yleisimpiä uhkia ja trendejä, kertomalla tärkeimpiä lakeja ja viitekehyksiä sekä esittelemällä tässä tutkimuksellisessa kehittämistyössä tutkimusmenetelmänä käytetty Kyberturvallisuuskeskuksen kybermittari -työkalu. Luvussa 5 perehdytään keinoihin, joiden avulla voidaan yrityksissä parantaa kyberturvallisuutta, ja joihin olisi hyvä keskittyä. Seuraavaksi luvussa 6 sovelletaan aiempaa teoriaa ja mennään itse tutkimukselliseen kehittämistyöhön. Aluksi esitellään käytetyt menetelmät ja sitten teemahaastattelun ja kybermittarin tulokset. Lopuksi vielä nykytila-analyysi tiivistetään SWOT-nelikenttämalliin ja annetaan kehitysehdotuksia ja jatkotoimenpiteitä. Tutkielman viimeisessä luvussa sidotaan langat yhteen ja esitetään yhteenveto ja loppupäätelmät.

2 Tutkimuksellisen kehittämistyön lähtökohdat

2.1 Kohdeorganisaatio

Kehittämistyön yhteistyökumppanina toimii matkailu- ravintola- ja tapahtuma-alan yritys, joka tuottaa kokonaisvaltaisia erä-, ravintola- ja tapahtumaelämyksiä tilauksesta. Yrityksen kohderyhmänä ovat suuret yritykset, joille järjestetään esimerkiksi asiakastilaisuuksia, seminaareja ja TYKY-päiviä, mutta myös yksityishenkilöille järjestetään erilaisia tilaisuuksia, kuten häitä ja hautajaisia. Yrityksen tapahtumakeskuksessa järjestetään esimerkiksi kesäteatteria ja eri artistien konsertteja. Lisäksi yritys järjestää eräelämysmatkoja metsästyksen ja kalastuksen parissa ympäri Suomea.

Yrityksessä työskentelee keskimäärin 20 henkilöä, joista 6 työskentelee päivittäin tietokoneella. IT-tuen yritys on ulkoistanut erilliselle tietopalveluyhtiölle. Yritys käsittelee päivittäin paljon henkilö- ja yritystietoja esimerkiksi varatessaan asiakkaille lentolippuja ja muita matkapalveluita tai tapahtumalippuja tai ottaessaan muita varauksia vastaan. He ylläpitävät myös suurta asiakasrekisteriä.

Yritykseen on viime aikoina kohdistunut monenlaisia huijausyrityksiä. Heidän nimissään on luotu virheellisiä Facebook tapahtumia, yritetty saada asiakkaita painamaan vääriä linkkejä, lähetetty asiakkaille yrityksen nimellä huijausviestejä sekä yritys on saanut uhkailuviestejä, joissa on vaadittu lunnaita. Kohdeyrityksessä ei ole kuitenkaan aiemmin juurikaan kiinnitetty huomiota kyberturvallisuusasioihin eikä heillä ole ennalta paljon tietoisuutta, kuinka heidän

tulisi toimia esimerkiksi edellä mainittujen huijausyritysten suhteen. Nyt kohdeyritys kuitenkin näkee tarpeelliseksi kehittää tapoja ennalta ehkäistä huijausyrityksiä sekä toimintatapoja reagoida näihin. Yrityksen toimiala ja koko huomioiden, täytyy kehittämistyössä muistaa, että kyberturvallisuutta ei voi nostaa liian suurelle jalustalle yrityksen toiminnassa, ja täytyy ottaa huomioon pienen yrityksen budjetti ja resurssit tällaiseen kehittämistyöhön.

2.2 Työn tausta ja perusteet

Kyberturvallisuus on hyvin ajankohtainen ja pinnalla oleva aihe. Maailman digitalisoituminen jatkuu kovaa vauhtia ja yhä enemmän ja enemmän erilaisia laitteita kytkeytyy verkkoon. Myös kyberuhkien määrä lisääntyy koko ajan. Koronaviruspandemia paljasti etätyöbuumin kautta uudenlaisia kyberuhkia ja Venäjän hyökättyä Ukrainaan on erilaiset kybersodan muodot nousseet pinnalle. Kaikki eivät kuitenkaan ole vielä ymmärtäneet kyberriskien merkitystä ja suojautumisen tärkeyttä niitä vastaan. Opinnäytetyössäni aion tuoda esiin, kuinka jokaisen tulisi kiinnittää ainakin jollain tasolla kyberturvallisuuteen huomiota, viimeistään nyt.

Kyberturvallisuus on mielenkiintoinen aihe ja suhteellisen uusi, mistä ei vielä löydy tutkimusta vuosisatojen takaa eikä yhteiset termit ja tutkimustavat ole vielä vakiintuneet. Olen koko opintojen ajan ollut kiinnostunut kyberturvallisuudesta ja varsinkin kun aihe on noussut yhä enemmän ajankohtaiseksi, tiesin haluavani tehdä opinnäytetyöni tähän liittyen. Tulevaisuudessa haluaisin myös mahdollisesti työskennellä kyberturvallisuuden parissa.

Halusin löytää yhteistyöyritykseksi sellaisen organisaation, jossa kyberturvallisuusasioita ei vielä ole otettu juurikaan huomioon, jotta voisin auttaa heitä laittamaan perusasiat kuntoon. Halusin myös pienen yrityksen, joka ei välttämättä suoraan vaikuta selkeimmältä hyökkäyksen kohteelta voidakseni tuoda esiin sitä, kuinka kuitenkin kaikkien tulisi ottaa kyberturvallisuusasiat huomioon, kaiken kokoisten yritysten ja kaikilta aloilta. Opinnäytetyön aihe syntyi kohdeyrityksen kanssa yhteisestä tarpeesta: minä halusin tehdä opinnäytetyön kyberturvallisuuteen liittyen ja kohdeyritys taas tarvitsi kiperästi apua näissä asioissa.

2.3 Tarkoitus ja tavoite

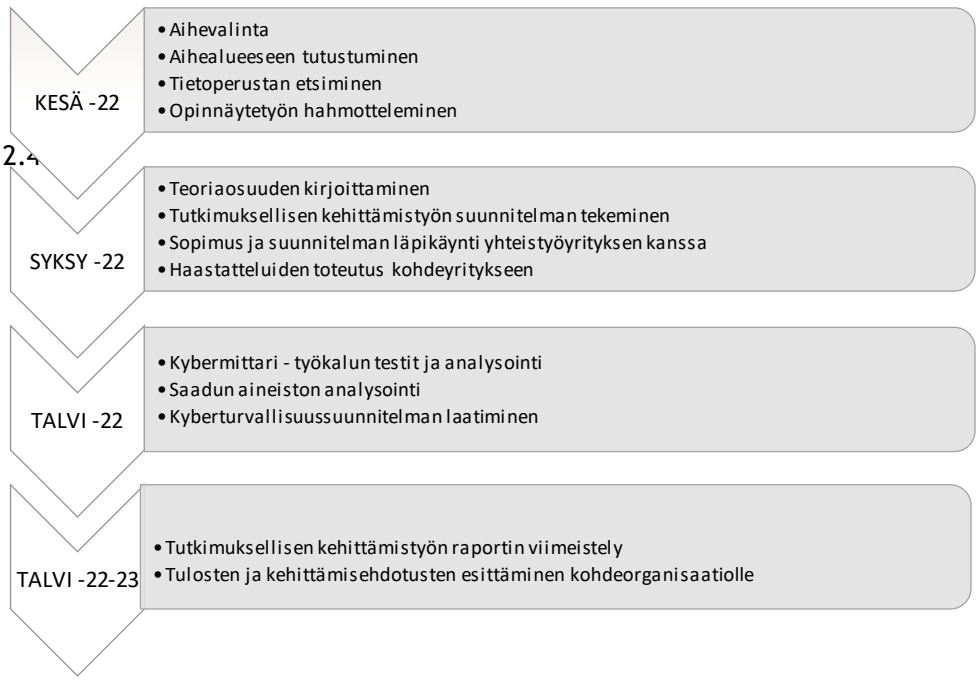
Opinnäytetyön tarkoituksena on selvittää kohdeyrityksen kyberturvallisuuden lähtötaso sekä siihen vaikuttavat tekijät, ja antaa ohjeistukset ja toimenpiteet kyberturvallisuuden kehittämiseksi ja ylläpitämiseksi. Aluksi yrityksen kyberturvallisuuden nykytila selvitetään johdon haastatteluiden sekä Traficomin kyberturvallisuuskeskuksen kybermittari -työkalun avulla, ja näiden sekä laajan teoriakatsauksen pohjalta luodaan kyberturvallisuuden nykytila-analyysi SWOT-nelikenttämalliin, jonka jälkeen esitetään kehitysideoita ja jatkotoimenpiteitä yrityksen tarpeisiin. Tarkoituksena on nostaa esiin kyberturvallisuuden ja kyberriskeihin varautumisen merkitystä, ja tuoda esiin miksi myös pienten yritysten suojaaminen ja kyberturvallisuuden suunnitteleminen on tärkeää, ja sellaistenkin yritysten, jotka ei suoraan ole niin

merkittävä tai selkeitä hyökkäyksen kohteita. Haluan painottaa sitä, että kaikilla yrityksillä tulisi olla jonkinnäköinen kyberturvallisuussuunnitelma sekä nykytilanne tiedossa. Motiivinani on oman, yrityksen sekä yleisesti kaikkien kybertietotason nostaminen, ja päästä lähemmäksi sellaista tavoitetilaa, jossa jokainen tietäisi mitä kyberturvallisuus on, ja ymmärtäisi sen olevan osa meidän jokaisen elämää, ja että kyberuhkia vastaan pitää suojautua.

Työn tavoitteena on kehittää kohdeyrityksen kyberturvallisuutta ja kybertietoisuutta, ja antaa heille peruslähtökohdat ja välineet suojautua kyberhyökkäyksiltä ja niiden haitallisilta vaikutuksilta. Tavoitteena on, että tekemäni nykytila-analyysin avulla yritys saa hyvän käsityksen lähtötasostaan ja tämän avulla saada kyberturvallisuuden perustason toimenpiteet kuntoon sekä valjastettua kyberturvallisuuden osaksi yrityksen arkea.

Aikataulu

2.4



Kuvio 1: Aikataulu

Kuviossa 1. näkyy opinnäytetyön aikataulusuunnitelma. Tutkimuksellinen kehittämistyö aloitettiin loppukesästä 2022 tutustumalla aiheen lähdekirjallisuuteen ja hahmottelemalla kehittämistyön kokonaisuutta sekä aihealueen rajausta. Ensimmäinen yhteydenpito kohdeyritykseen oli elokuussa, jossa yhdessä käytiin läpi tutkimuksellisen kehittämistyön tarkoitusta ja tavoitetta. Heti alkusyksystä pääsin kirjoittamaan teoriapohjaa ja laatimaan tarkemman kehittämistyön suunnitelman ja sopimuksen yhteistyöyrityksen kanssa. Marraskuun aikana toteutettiin haastattelu yritysjohdolle sekä tämän jälkeen joulukuussa suoritettiin kybermittari -

työkalun testaukset. Joulukuussa laadin vielä alustavat tulokset sekä hahmottelin kehittämissuunnitelmaa. Alkuvuodesta 2023 viimeistelin tulosten analysoinnin ja raportin sekä esittelin nämä kohdeyritykselle.

3 Kyberturvallisuuden käsitteitä

3.1 Mitä on kyberturvallisuus?

Turvallisuus on jokaisen ihmisen yksi perustarpeista. Se muuttuu ja elää maailman mukana eikä ole pysyvä tila eikä täydellistä turvallisuutta olekaan olemassa. Turvallisuus voidaan ajatella vaaran tai riskin poissaolona. Turvallisuutta uhkaavaa vaaraa ei yleensä voi kokonaan poistaa, vaan kyse on riskin vähentämisestä ja siitä paljon siihen halutaan panostaa. Kyberturvallisuus on hyvä esimerkki siitä, kuinka turvallisuus voi nopeastikin muuttua ja syntyä kokonaan uusia ulottuvuuksia, joita turvallisuudessa täytyy ottaa huomioon. (Limnéll, Majewski & Salminen 2014, 27.)

Kyber tarkoittaa digitaalista, bittien maailmaa ja se yhdistää datan, informaation ja tiedon käytön (Limnéll ym. 2014, 29). Kyberturvallisuus taas on tavoitetila, jota kohti pyritään lisäämällä erilaisia toimia. Kyberturvallisuus on siis bittien maailman turvallisuutta, se on digitaalisen maailman tila, jossa vallitsee ymmärrys ja luottamuksen tunne siitä, että tehdyillä ennakoivilla toimenpiteillä kyetään sietämään kyberuhkia ja niiden vaikutuksia. Kyberympäristö on turvallinen silloin, kun sen toimintaan voi luottaa. Koko yhteiskuntamme on riippuvainen kyberturvallisuudesta esimerkiksi sähköverkko, pankkijärjestelmä sekä energiajakelu, ja on vaikea kuvitella yhteiskuntaa tai yritysten palveluja ilman digitaalista bittien maailmaa. (Limnéll ym. 2014, 39.)

Kyberturvallisuus voidaan määritellä tietoteknisen infrastruktuurin verkostoksi, joka sisältää Internetin, tietoliikenteen verkot, tietokonejärjestelmät sekä eri prosessori- ja ohjelmateollisuuden alat (Allison 2014, 18). F-Secure (2022 a) määrittelee kyberturvallisuuden kattavan kaiken ohjelmistoista niihin toimiin, joilla pyritään turvaamaan eri laitteita ja tietoa hyökkäyksiltä, häiriöiltä ja muilta vaaroilta. Traficomin kyberturvallisuus ja yrityksen hallituksen vastuu -opas (2020, 3-4) taas määrittelee kyberturvallisuuden tarkoittavan yhteiskunnan ja organisaatioiden digitalisoitumisen myötä syntyneitä uudenlaisia turvallisuushaasteita ja niitä toimenpiteitä, joilla yritykset suojaavat liiketoimintansa tärkeät järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet. Se on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta on turvattu (Kybermittari Kansallinen kyberturvallisuuden…2020, 33).

Microsoft (2022) rinnastaa kyberturvallisuuden termin digitaaliseen turvallisuuteen ja määrittelee sen tarkoittavan tapoja, joilla suojataan digitaalisia tietoja, laitteita sekä resursseja. Se

sisältää esimerkiksi henkilötiedot, tilit, tiedostot, valokuvat ja rahat. Microsoft määrittelee myös kyberturvallisuuden kolme peruspilaria, joita tavallisesti on käytetty myös tietoturvallisuuden peruspilareina ja tavoitteina, nämä ovat: luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa, ettei kenelläkään saa olla pääsyä yksityisiin ja luottamuksellisiin tietoihin. Eheydellä taas viitataan käytettävien järjestelmien ja niiden tietojen virheettömyyteen, ettei tietoja pääse luvattomasti muokkaamaan ja saatavuudella taas sitä, että valtuutetut käyttäjät pääsevät ongelmitta ja nopeasti tarvittaviin tietoihin käsiksi.

Yrityksille kyberturvallisuus tarkoittaa ennen kaikkea toimintavarmuutta, jonka avulla suojaudutaan ikäviä tekijöitä vastaan ja ennalta ehkäistään ja torjutaan niitä sekä lievennetään niiden vaikutuksia. Kyberturvallisuutta ei pidä kuitenkaan nähdä pelkkänä negatiivisena uhkana, vaan parhaimmillaan se tehostaa ja laajentaa yrityksen toimintaa ja tarjoaa uusia mahdollisuuksia ja luo uutta kehitystä. Kyberturvallisuuden varmistaminen on tulevaisuuden toiminnan varmistamista. (Limnéll ym. 2014, 57-58.)

3.2 Kyberturvallisuus vs. tietoturvallisuus

Kyberturvallisuus on käsitteenä hyvin laaja ja se sekoitetaan usein tietoturvaan, mutta kyberturvallisuus on paljon muutakin kuin tietojen turvaamista. Se sisältää sen lisäksi esimerkiksi myös liiketoiminnan turvaamista, riskienhallintaa sekä ihmisten koulutusta ja perehdyttämistä. Jotta kyberturvallisuus voi olla kunnossa, pitää kuitenkin myös tietoturvallisuuden olla kunnossa. (Isotalo 2018.) Kyberturvallisuudesta ja tietoturvallisuudesta saatetaan monesti helposti puhua ikään kuin synonyymeina, vaikka ne eivät tätä ole. Siinä missä kyberturvallisuus keskittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden turvaamiseen verkkoympäristössä, niin tietoturvallisuus kattaa tiedon turvaamista myös fyysiseen tallentamiseen liittyen sekä digitaalisen ympäristön ulkopuolella. Tietoturva viittaa siis tietojen turvaamiseen, olivatpa ne sitten digitaalisessa tai fyysisessä muodossa. Myös kyberturvallisuuden ja tietoturvallisuuden uhat ovat hieman erilaisia. Kyberturvallisuus keskittyy torjumaan haittaohjelmien kaltaisten haittojen aiheuttamia vahinkoja, kun taas tietoturva myös tiedon levittämisen sekä väärän tiedon torjuntaa. (F-Securite 2022 a.)

Yrityksissä monesti tietoturva on tunnetumpi käsite kuin kyberturva. Tietoturva turvaa yrityksen tietopääomaa, jota voivat olla esimerkiksi aineettomat oikeudet, kuten patentit ja tekijänoikeudet, tietokannat, asiakastiedot ja sopimustekstit. Tavoitteena on turvata tiedon säilyminen, saatavuus, liikuteltavuus, yhtenäisyys ja luottamuksellisuus. Tietoturvan ylläpito vaatii ymmärrystä digitaalisten laitteiden käyttäjistä, järjestelmistä ohjelmistoineen ja fyysisestä verkkoinfrasta, jossa data liikkuu. Ihmisten ja bittien yhteen muodostuneessa kybermaailmassa pelkkä tietoturva ei kuitenkaan enää riitä vaan tarvitaan kokonaisvaltaisempaa kyberturvallisuutta. (Limnéll ym. 2014, 55-56.)

Myös tietosuoja sekoitetaan monesti tietoturvallisuuteen. Tietosuojalla tarkoitetaan henkilötietojen keräämiseen, säilyttämiseen ja käyttöön liittyviä asianmukaisia tapoja ja lakeja. Yksityisyyden suojan tulee toteutua myös verkossa ja tietojen pysyä turvassa ilman, että niihin päästään käsiksi. (F-Securite 2022 a.)

3.3 Kybertoimintaympäristö

Digitaalinen liiketoimintaympäristö on muuttanut asiakkaiden odotuksia ja liiketoimintamalleja. Se on muuttanut yritysten tapaa keskustella, käyttäytyä ja verkostoitua asiakkaiden sekä muiden yritysten, kumppaneiden ja toimittajien kanssa. Se on myös lisännyt liiketoiminnan vauhtia ja on muuttanut ihmisten ja tavaroiden kohtaamista sekä liiketoimintastrategioita, ja vienyt koko liiketoimintaympäristön verkostoituneeseen digitaaliseen liiketoimintajärjestelmään. Digitaalinen liiketoiminta muokkaa myös tulevaisuutta, ja yritysten täytyy kehittää jatkuvasti liiketoimintaekosysteemiään ja teknologioita pysyäkseen kilpailukykyisinä. Digitaalisen toimintaympäristön haasteita ovat liiketoiminnan kannalta kriittisten tietojen hallinnointi, tehokas ja turvallinen tietojensiirto sekä jatkuvasti ja nopeasti kehittyvän digitaalisen ympäristön perässä pysyminen. (Nayyar, Rameshwar, & Solanki 2020.)

Kybertoimintaympäristö on globaali egosysteemi, jonka palasia yhteiskunnan eri järjestelmät ja toimijat ovat, ja joka kasvaa ja kehittyy koko ajan. Se muodostuu informaatioinfrastruktuurista, joka sisältää esimerkiksi keskenään vuorovaikutuksissa olevat ja verkottuneet yritykset, valtiot, yksilöt, prosessit, teknologiat ja kaiken sen mikä vaikuttaa näiden kyberturvallisuuteen. Yrityksessä digitaalinen maailma läpäisee koko yrityksen toiminnan aina myynnistä palkanlaskentaan. Kyberturvallisuus on yhdistynyt osaksi kokonaisturvallisuutta. (Limnéll ym. 2014, 74-75.)

Kybertoimintaympäristö voidaan määritellä digitaalisista tietojärjestelmistä muodostuvaksi kokonaisuudeksi, jossa organisaation tiedonkäsittelyä toteutetaan. Se rakentuu yrityksen teknisistä ja teknologisista valinnoista, toimialan erityispiirteistä sekä yhteyksistä yrityksen ulkopuolisiin sidosryhmiin kuten viranomaisiin, sopimuskumppaneihin ja sen asiakkaisiin. (Kybermittari Kansallinen kyberturvallisuuden…2020, 33.) Turvallisessa kybertoimintaympäristössä arki sujuu ilman suurimpia häiriöitä, ja ihmiset osaavat toimia ilman turhia virheitä, toiminta on ennakoivaa, ollaan ajan tasalla maailman tapahtumista, työntekijät ovat perillä omista vastuistaan ja kaikki osaavat ilman paniikkia toimia häiriötilanteissa. (Limnéll ym. 2014, 44.)

Ulkoministeriö (2022) määrittelee kybertoimintaympäristön ihmisten luomaksi digitaaliseksi rinnakkaistodellisuudeksi, mikä globaalisti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta ihmiset ja laitteet toisiinsa maailmanlaajuisesti. On hyvä tiedostaa, että niin yksittäisen yrityksen kuin koko yhteiskunnan kannalta monet elintärkeät toiminnot ovat myös riippuvaisia digitaalisista verkoista, kuten esimerkiksi teollisuus, vesi- ja energiahuolto, pankkijärjestelmä-, terveydenhuolto ja

liikenne. Kyberturvallisuudesta huolehtimalla varmistetaan, ettei kyberympäristöstä aiheudu haittaa, vaaraa tai häiriötä siitä riippuvalle toiminnalle.

Globaali laaja kyberturvallisuusympäristö luo uusia mahdollisuuksia, mutta myös paljon uudenlaisia uhkia. Verkossa liikkuvat suuret rahamäärät houkuttelevat kyberrikollisia etsimään koko ajan uusia tapoja ansaita rahaa. Kyberrikollisuudessa liikkuu todella suuria rahasummia. (Isotalo 2018.) Toimintaympäristöä ei voi myöskään rajata pelkästään kotimaahan, sillä Kyberuhat leviävät digitaalisessa globaalissa verkossa helposti valtioiden rajojen yli. Keskeinen tekijä kyberturvallisuuden kansainvälisessä yhteistyössä on ulkoministeriö. EU:n ohella kybertoimintaympäristökeskustelua käydään muun muassa YK:ssa, Etyj:ssä, Euroopan neuvostossa, OECD:ssä ja Natossa. (Ulkoministeriö 2022).

Yritysten tulisi jatkuvasti seurata toimintaympäristön muutoksia ja ajankohtaisia asioita. Venäjän hyökättyä Ukrainaan ja Suomen jätettyä Nato hakemus, on kyberturvallisuus noussut entistä merkittävämmäksi uusien uhkien myötä, ja on nyt todellakin ajankohtainen aihe. Traficomin kyberturvallisuuskeskus (Kyberturvallisuuden vahvistaminen suomalaisissa…2022) on luonut uuden ohjeen suomalaisille yrityksille kyberturvallisuuden vahvistamiseen muuttuneen kansainvälisen tilanteen myötä. Ohjeistuksessa muistutetaan johtoa myös olevan tavoitettavissa ja valmiina mahdollisten kriittisten päätösten tekemiseksi sekä seuraamaan oma-aloitteisesti viranomaisten tiedotteita kyberturvallisuuden tilasta.

3.4 Kybertuvallisuusriski ja kyberuhka

Uhka on toimintaympäristössämme havaittu vaara, haitta tai epävarmuustekijä. Uhka voi olla mikä tahansa yritystoiminnan kannalta kielteinen asia, joka voi aiheuttaa vahinkoa tai estää toimintaa. Kyberuhka on digitaalisessa maailmassa tapahtuva turvattavan kohteen turvallisuutta vaarantava tekijä, joka voi olla joko tahallisesti tai tahattomasti aiheutettu. Tekniset viat, ohjelmistovirheet tai vaikka syysmyrskyt ovat esimerkkejä mahdollisista kyberuhista. (Limnéll ym. 2014, 34, 37.)

Uhkia voidaan torjua, mutta riskiä ei, vaan se sisältyy aina kaikkeen toimintaan. Riski on negatiivisen tapahtuman mahdollisuus tulevaisuudessa. Todennäköissyyslaskennalla voidaan arvioida eri riskien todennäköisyyksiä ja sen toteutumisen vaikutuksia. Torjumisen sijaa riskejä voidaan kuitenkin välttää, omaksua, rajata, lieventää tai siirtää niitä sekä oppia elämään niiden kanssa. (Limnéll ym. 2014, 108.) Kyberriskeillä tarkoitetaan informaatioteknologiasta aiheutuvia taloudellisen tappion, maineen vahingoittumisen tai muun häiriön riskejä, jotka aiheuttavat yritykselle vahinkoa. Riskien tiedostamisella pyritään minimoimaan vahingot ja ei toivotut seuraukset. (Williams 2014, 10.)

Kyberriskejä syntyy monista eri syistä ja lähteistä kuten järjestelmävirheistä, ihmisten toimenpiteistä, sisäisten prosessien epäonnistumisesta tai jostakin ulkoisesta tapahtumasta.

Kyberriskit voivat toteutua joko tahallisten ja luvattomien tietoturvaloukkauksien seurauksena, kun rikolliset tunkeutuvat tietojärjestelmiin tarkoituksenaan vakoilu, kiristäminen tai vain hämmennyksen aiheuttaminen. Tai kyberriskit voivat toteutua myös esimerkiksi tahattomien tai vahingossa aiheutuneen turvallisuusrikkomusten seurauksena tai sitten järjestelmien huonon eheyden vuoksi. (Williams 2014, 10.) Kyberturvallisuusuhkana voidaan pitää myös ihmisten inhimillisiä virheitä ja huolimattomuutta. Merkittävä uhka on myös internetissä toimiva rahaliikenne, joka tarjoaa verkkorikollisille mahdollisuuksia päästä käsiksi esimerkiksi pankkitietoihin. (F-Secure 2022 a.)

Kyberriskit ovat koko ajan kovaa kasvava uhka. Kyberrikolliset voivat olla soluttautuneena yrityksen järjestelmiin jopa vuosien ajan huomaamatta. Yritysten on tärkeä ymmärtää mitkä ovat sen tärkeimmät kyberriskit, miten niitä voidaan havaita ja miten suojautua näitä vastaan sopivalla kustannustasolla. Kyberriskin toteutuessa on yleensä kyse tärkeiden yritystietojen, immateriaalioikeuksien tai asiakkaiden taloudellisten tietojen menettämisestä. Seuraukset voivat olla taloudellisesti merkittäviä tai yritys voi saada sakot, menettää maineensa tai joutua jopa hetkellisesti keskeyttämään toimintansa. (Allison 2014, 4.)

4 Syvemmälle kyberturvallisuuteen

4.1 Yleisimmät kyberriskit ja trendit

Yleisimpiä kyberriskejä ovat tietojenkalastelu, haittaohjelmat, palvelunestohyökkäykset. Tietojenkalastelu on yksi yleisempiä kyberriskejä. Tässä kyberrikollisten tarkoituksena on saada haltuunsa käyttäjätunnus- ja salasanapareja sekä muita yrityksen tärkeitä tietoja, kuten maksukorttitietoja. Varastetuilla tunnuksilla rikolliset voivat päästä vakoilemaan monenlaisia yrityssalaisuuksia, ja tähän voi lisäksi myös liittyä maine- ja sääntelyriskejä. (Kyberturvallisuus ja yrityksen… 2020, 4-6.) Tietojenkalastelua toteutetaan usein sähköpostilla lähettämällä aidon oloinen tietojenkalasteluviesti esimerkiksi pankilta tai esimieheltä, ja näin yritetään saada tietoon esimerkiksi pankkitietoja tai maksamaan valelasku. Tai sitten pyritään saamaan uhri painamaan haitallista linkkiä, joita liikkuu sähköpostin lisäksi myös tekstiviestitse, eri verkkosivuilla ja sosiaalisessa mediassa. (Pienyritysten kyberturvallisuusopas 2020, 4.) Tietojenkalastelussa luovutat siis käytännössä itse verkkorikollisille heidän tarvitsemansa tiedot, joten tässä tapauksessa ei edes antivirusohjelmasta ole apua. Asiakkaiden tietoja säilyttävien yritysten on lisäksi varauduttava tietomurtoihin – ja vuotoihin, sillä näissä hyökkääjät pyrkivät pääsemään käsiksi useiden ihmisten henkilökohtaisiin tietoihin, ja tällä voi olla suuria taloudellisia seurauksia sekä mainehaitta. (F-secure 2022 b.)

Haittaohjelma on ohjelmisto, jonka tarkoituksena on aiheuttaa harmia tai tuoda taloudellista hyötyä rikolliselle. Haittaohjelmia ovat esimerkiksi virukset, vakoiluohjelmat, troijalaiset ja

madot. Rikolliset voivat esimerkiksi asentaa haittaohjelman varastamaan tärkeätä tietoa tai ottaa tietokone käyttöönsä tai vakoilla käyttäjää. (Pienyritysten kyberturvallisuusopas 2020, 7.) Haittaohjelmat leviävät monesti sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivustojen sekä haavoittuvien palvelinten kautta. Maailmanlaajuisesti yleistyneessä ilmiössä, Big Game Hunting:ssa, rikolliset pyrkivät tunkeutumaan erityisen houkuttelevien ja varakkaiden yritysten järjestelmiin ja levittäytymään sen verkkoon. Sitten kyberhyökkääjät pyrkivät lamauttamaan yrityksen toiminnan kiristyshaittaohjelmalla ja kiristävät maksamaan lunnaita haittaohjelman purkamiseksi. (Kyberturvallisuus ja yrityksen… 2020, 6.)

Palvelunestohyökkäyksen eli DOS (Denial of Service) tarkoituksena on kaataa yrityksen verkkosivut tai estää käyttäjien pääsy kokonaan niille. Verkkosivujen toimintaa häiritään kohdistamalla sivuille normaalia huomattavasti paljon enemmän verkkoliikennettä, jota verkkosivut eivät pysty enää hallitsemaan. Palvelunestohyökkäykseen voi yksittäisen hyökkääjän sijaan osallistua myös lukuisia internetiin yhdistettyjä laitteita, jolloin puhutaan hajautetusta palvelunpalvelunestohyökkäyksestä DDoS (Distributed Denial of Service). Tämä toteutetaan usein tähän tarkoitukseen suunnitellulla ohjelmalla ja hyödyntämällä verkostoon kaapattuja laitteita eli botnettiä. Botnettin kuuluvat laitteet lähettävät sitten jatkuvasti pyyntöjä ja verkkoliikennettä hyökkäyksen kohteena olevalle verkkosivulle. Verkkoon liitettyjä laitteita voivat olla tietokoneiden lisäksi esimerkiksi reitittimet, muut mobiililaitteet tai vaikka verkkoon liitetty kamera. Lukuisten laitteiden avulla voidaan saada suurta vahinkoa aikaiseksi ja näitä on myös vaikeampi torjua ja jäljittää. (F-secure 2022 b.)

Tuorein selvästi esiin noussut esimerkki palvelunestohyökkäyksestä Suomessa on huhtikuussa 2022 valtioneuvoston ja ministeriöiden verkkosivuja vastaan kohdistunut hyökkäys, jonka oletetaan olevan osa Venäjän kybersodankäyntiä. Hyvä esimerkki suuresta botnet-verkosta taas on Mirai, joka oli poikkeuksellisen laaja verkosto koostuen sadoista tuhansista IoT- eli Internet of Things -laitteista, kuten esimerkiksi kodinelektroniikasta ja reitittimistä. Mirai-verkoston hyökkäyksen kohteeksi joutuivat esimerkiksi Twitter, Netflix ja Spotify. (F-secure 2022 b.)

Euroopan unionin kyberturvallisuusvirasto ENISA (Enisa Threat Landscape…2021, 4-10) on listannut tarkastelujaksolla huhtikuu 2020 - heinäkuu 2021 havaitut merkittävimmät kyberuhat ja trendit. Yleisesti kyberhyökkäyksien ja erilaisten kyberuhkien määrä on jatkanut kovaa kasvuaan, kuten myös niiden haitalliset vaikutukset. Hyökkäykset ovat yhä kehittyneempiä, monimutkaisempia ja vaikuttavampia ja vaikeammin havaittavissa ja torjuttavissa. ENISA:n raportissa suurimmaksi uhaksi 2020-2021 nousee ransomware-hyökkäykset, jotka ovat eräänlaisia kiristyshaittaohjelmia, jotka lukitsevat laitteet tai tiedot kokonaan, ja tämän jälkeen kyberrikolliset vaativat maksamaan lunnaita bitcoineina tietojen vapauttamiseksi. Selkeäksi trendiksi on noussutkin hyökkäysten motiivina raha, kuten lunnasvaatimukset sekä erityisesti kryptovaluutan käyttäminen näissä. Myös kryptojacking-hyökkäysten määrä, eli erilaisten laitteiden luvaton käyttö kryptovaluutan louhimiseen, oli ennätyskorkea 2021 vuonna. COVID-19-

pandemia on selvästi vaikuttanut kyberturvallisuusympäristöön. Sähköpostihyökkäyskampanjat sekä muut kotitoimistoihin tehdyt hyökkäykset ovat olleet merkittävä uusi uhka ja inhimillisten virheiden määrä on selvästi noussut COVID-19-pandemian seurauksena jopa niin, että useimmat murrot vuonna 2020 johtuivat juurikin ihmisten tai järjestelmien määritysten virheistä. Yrityksiin kohdistetut sähköpostihuijaukset ovat lisääntyneet ja kehittyneet entisestään. ENISA nostaa esiin merkittävänä uhkana myös toimitusketjuihin kohdistuvat uhat. Palveluntarjoajista on tullut arvokkaita hyökkäyskohteita kyberrikollisille ja hyökkäykset toimitusketjuihin on suuressa nousussa. Lisäksi ENISA mainitsee esimerkiksi terveydenhuoltoalaan liittyvien tietomurtojen lisääntyneen sekä disinformaation levittämisen.

Kyberturvallisuus on kovaa kehittyvä ala ja sen merkitys kasvaa koko ajan uudenlaisten tapahtumien ja elektroniikan kehityksen myötä. F-Secure (2022 a) listaa artikkelissaan 2022 vuoden kyberturvallisuuden trendejä ja mainitsee ensimmäisenä 2020 alkaneen COVID-19-epidemian, jonka seurauksena etätöistä on tullut uusi trendi, ja verkkorikolliset ovat näin löytäneet uusia väyliä päästä yritysten tietoihin ja järjestelmiin käsiksi. Toinen 2022 selvästi pinnalla oleva aihe on maailmanpolitiikasta heijastuvat tapahtumat kyberturvallisuuteen. Toiseksi trendiksi voidaan määritellä kybersodankäynti, jonka kohteena ovat erityisesti valtion toiminnan kannalta kriittinen infrastruktuuri. Valtioiden tulee valmistautua myös ulkopuoliseen tiedusteluun, vakoiluun sekä disinformaation levittämisen torjumiseen. F-Secure mainitsee kolmanneksi trendiksi esineiden internetin eli IoT:in (Internet of Things) ja tätä myötä yhä useampien laitteiden ja kuluttajatuotteiden yhdistymisen verkkoon. Kun yhä useammat kodinkoneet, kuten uunit ja jääkaapitkin on yhdistettynä internetiin, kasvavat myös riskit, sillä laitteiden älyominaisuudet tekevät laitteista haavoittuvaisia ja potentiaalisia kyberhyökkäyksien kohteita. Monia IoT-laitteita on esimerkiksi käytetty osana palvelunestohyökkäyksiä.

Digitalisaatio ja sen tuomat uudet toimintatavat ovat tuoneet valtavien hyötyjen ja mahdollisuuksien lisäksi myös uusia riskejä. Esimerkiksi pilvipalvelut, esineiden internet ja sosiaalinen media ovat tuoneet uusien liiketoimintamahdollisuuksien lisäksi myös uusia riskejä ja väyliä rikollisille päästä käsiksi yrityksen tietoihin. Yrityksille onkin suuri haaste pysyä nopeasti muuttuvan maailman perässä samalla hyödyntäen uusia mahdollisuuksia, mutta kuitenkaan jäämättä kehityksen jalkoihin ja huomioiden myös uudet haasteet. Sosiaalinen media on tuonut valtavia muutoksia henkilökohtaiseen, sosiaaliseen ja liike-elämäämme ja se voi tarjota valtavia mahdollisuuksia tai aiheuttaa suurta vahinkoa organisaatioille. Mobiililaitteista on tullut osa jokapäiväistä elämäämme, ja liiketoiminnan ja henkilökohtaisen käytön rajat ovat hämärtyneet, mikä vaikuttaa yritysten turvallisuuteen. Monet yritykset ovat sallineet työntekijän henkilökohtaisen puhelimen käytön työkäyttöön, mutta vain harva on ottanut huomioon sen tuomat turvallisuusuhat. Yritysten täytyykin löytää tasapainon sen välillä, mitä käyttäjät haluavat, ja mikä taas on yrityksen ja turvallisuuden kannalta parasta. (Williams 2014, 11.) Lisäksi yksi yrityksen sisältä kumpuava uhka on työntekijöiden huolimattomuus, tietämättömyys sekä tyytymättömyys ja he voivat joko tahattomasti tai tahallisesti aiheuttaa

merkittäviä riskejä, joiden toteutumisella voi olla suuria vaikutuksia niin talouteen, maineeseen kuin tietopääomaan. (Limnéll ym. 2014, 107.)

Kyberriskit ovat suhteellisen uusia eikä monilla organisaatioilla ole vielä kokemusta niiden ymmärtämisestä. Turvallisuuteen investoiminen voi myös olla kallista, ja monet yritykset jättävätkin investoinnit turvallisuuteen tekemättä. He saattavat ajatella ettei tarvitse, koska yritykseen ei aiemminkaan ole hyökätty tai etteivät kyberriskit koske heitä tai ettei heillä ole mitään, mitä hyökkääjät haluavat. Kukaan ei kuitenkaan ole immuuni. Kaiken kokoiset ja tyyppiset yritykset ovat potentiaalisia hyökkäyskohteita, myös pienet yritykset. Rikolliset hyökkäävät monesti juuri niihin yrityksiin, mitkä ovat vähiten suojattuja ja varautuneita, sillä ne ovat helppoja kohteita. Pienissä yrityksissä henkilöstön virheisiin liittyvät tapaukset ovat yleistyneet. (Williams 2014, 12; Allison 2014, 19-20.) Monet hyökkääjät valikoivat kohteensa täysin sattumanvaraisesti hyödyntämällä automatisoituja hyökkäyksiä tietojenkalasteluun, tietomurtoihin ja haittaohjelmien levittämiseen, jonka vuoksi jokainen yritys voi joutua kyberrikollisuuden uhriksi, vaikka ei pitäisikään itseään merkittävänä kohteena (F-secure 2022 a). 100 %:sta turvallisuutta on kuitenkin mahdotonta saavuttaa, vaan yritysten on pystyttävä reagoimaan tapauksiin tehokkaasti ja suojella mahdollisia hyökkäyskohteita mahdollisimman paljon (Allison 2014, 20).

4.2 Keskeiset lait ja toimijat

Kyberturvallisuuteen ja erityisesti tietoturvallisuuteen liittyy nykyään paljon myös erilaisia lakeja ja säädöksiä, joita täytyy noudattaa ja joiden puitteissa tulee toimia. Tähän liittyy myös useita viranomaistoimijoita, jotka säätävät asetuksia, valvovat, kehittävät ja auttavat kyberturvallisuus asioissa. Yrityksissä huomioitavia Suomen tietosuojalainsäädäntöjä ovat erityisesti: Tietosuojalaki (Tietosuojalaki 1050/2018), Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (Laki henkilötietojen käsittelystä 1054/2018), Laki sähköisen viestinnän palveluista (Laki sähköisen viestinnän palveluista 917/2014), Laki yksityisyyden suojasta työelämässä (Laki yksityisyyden suojasta työelämässä 759/2004) sekä Luottotietolaki (Luottotietolaki 527/2007). (Kyberturvallisuus ja yrityksen…2020, 42.)

Myös EU määrittelee kyberturvallisuuteen liittyviä asetuksia noudatettavaksi koko unionissa. EU:n verkko- ja tietoturvadirektiivissä, NIS-direktiivissä, säädetään tietoturvavelvollisuuksista sekä häiriöraportoinnista. Sääntelyllä velvoitetaan yhteiskunnan toimivuuden kannalta tärkeiden palveluntarjoajien tehdä tietoturvallisuusriskienhallintaa, turvaamaan palveluiden jatkuvuus ongelmatilanteessa sekä raportoimaan vastuuviranomaisille mahdollisista turvallisuuspoikkeamista ja uhista. Euroopan Unionin GDPR eli tietosuoja-asetus (Yleinen tietosuoja-asetus 2016/679) on tehty yksityisyyttä ja tietosuojaa turvaamaan. Siinä määrätään

henkilötietojen keräämiseen, säilyttämiseen ja hallinnoimiseen liittyvistä vaatimuksista. (Kyberturvallisuus ja yrityksen…2020, 42.)

Tärkeimmät viranomaiset ovat liikenne- ja viestintävirasto Traficomin kyberturvallisuuskeskus, poliisi, tietosuojavaltuutetun toimisto, huoltovarmuuskeskus ja poolit. Traficomin kyberturvallisuuskeskuksen tehtävänä on mm. kerätä tietoa kyberuhista ja tiedottaa tietoturva-asioissa sekä viestintäverkkojen ja viestintäpalvelujen toimivuuteen liittyvistä asioista. Se myös esimerkiksi valvoo ja ohjeistaa keskeisiä toimijoita ja tarkastaa ja hyväksyy järjestelmiä ja verkkoja. Poliisi pyrkii ennalta ehkäisemään ja selvittämään tietoverkkorikoksia sekä asettaa syytteeseen tarpeen tullen. Keskusrikospoliisiin on perustettu oma kyberrikostorjuntakeskus. Suojelupoliisissa taas tiedustellaan ja estetään kansalliseen turvallisuuteen kohdistuvia uhkia, kuten torjutaan Suomeen kohdistuvaa vakoilua sekä tuotetaan valtiojohdolle ja muille viranomaisille päätöksentekoa tukevaa turvallisuustietoa. Tietosuojavaltuutetun toimisto on viranomainen, joka valvoo tietosuojalainsäädännön ja henkilötietojen käsittelyä koskevien lakien noudattamista. Huoltovarmuuskeskus (HVK) ylläpitää ja kehittää Suomen huoltovarmuutta esimerkiksi hoitamalla valtion varmuusvarastointia sekä varmistamalla välttämättömien teknisten järjestelmien toimivuutta ja turvaa kriittistä tavara- ja palvelutuotantoa. Poolit taas vastaavat operatiivisesta varautumisesta yhdessä alan yritysten kanssa seuraamalla, selvittämällä ja suunnittelemalla ja valmistamalla toimenpiteitä omien alojensa huoltovarmuuden kehittämiseksi. (Kyberturvallisuus ja yrityksen…2020, 43.) Keskeinen tekijä kyberturvallisuuden kansainvälisessä yhteistyössä on ulkoministeriö. EU:n ohella kybertoimintaympäristökeskustelua käydään muun muassa YK:ssa, Etyj:ssä, Euroopan neuvostossa, OECD:ssä ja Natossa. (Ulkoministeriö 2022).

4.3 Viitekehys ja standardit

Yrityksen kyberturvallisuus on hyvä perustaa jonkin yleisesti tunnetun ohjeen pohjalle, joka antaa hyvät raamit kyberturvallisuuden hallinnalle. Hyviä viitekehyksiä kyberturvallisuudelle ovat esimerkiksi ISO 27000 -standardit, NIST kyberturvallisuuden viitekehys, Katakri-auditointikriteeristö sekä VAHTI- ohje. ISO 27001 (ISO/IEC 27001:2005) on kansainvälisesti laajasti tunnettu standardi, joka sisältää konkreettiset vaatimukset organisaation tietoturvan hallintajärjestelmälle. Ohjeistuksen avulla pyritään rakentamaan järjestelmä, joka suojaa organisaation tietoja ja kyberympäristöä. Ajatuksena on, että organisaatiosta tulee ennakoiva eikä reagoiva ja standardeja noudattamalla voi varmistaa käyttävänsä nykyaikaisia ja tehokkaita prosesseja riskeiltä suojautumiseen. ISO standardi antaa alusta loppuun asti prosessinomaiset raamit hyvän kyberturvallisuuden luomiseen, ja sisältää järjestelmän luomisen, käyttöönoton, hyödyntämisen, ylläpidon, valvonnan sekä kehittämisen peruselementit.

Tässäkin työssä käytettävä Kyberturvallisuuskeskuksen kybermittari -työkalu pohjautuu vahvasti NIST-viitekehykseen, joka on aikanaan luotu USA:n presidentin määräyksestä heidän

kriittisen infrastruktuurinsa suojaamiseen. NIST-viitekehyksen tarkoitus on tarjota yhteinen kieli kyberturvallisuusriskien ymmärtämiseen, hallintaan sekä kommunikointiin niin organisaation sisäisille kuin ulkoisille sidosryhmille. Se kokoaan yhteen kansallisesti hyväksi havaittuja toimintatapoja, joiden avulla yritykset voivat vertailla kehitystasoaan ja edistymistään kyberriskienhallintaa. NIST-viitekehys muodostuu neljästä osa-alueesta: toiminnot, kategoriat, alakategoriat ja viittaukset. Toiminnot edustavat kyberturvallisuuden elinkaarta ja ovat välttämättömiä kyberriskien hallinnassa, näitä toimintoja ovat: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen. Ensiksi tulee siis tunnistaa organisaation toiminnot, prosessit ja tietojärjestelmät, ja sitten riskienhallinnan kautta arvioida niiden kriittisyys ja suojaustarpeet. Kun tämä on tehty, toteutetaan tarvittavat suojaustoimenpiteet. Kriittisten toimintojen suojauksen ollessa kunnossa, havainnoidaan niiden toimintaa sekä tarvittaessa kehitetään suojausta lisää. Jos kyberuhka taas toteutuu, täytyy se havaita ajoissa ja reagoida siihen nopeasti. Palautuminen tapahtuu häiriöistä oppimisprosessin (lessons learned) avulla, jonka tarkoituksena on varmistaa, että haavoittuvuus on korjattu, prosessit ovat taas toimintakuntoisia ja että tapahtumasta on opittu. Jokaisella viitekehyksen toiminnoilla on lisäksi tarkentavia kategorioita sekä alakategorioita, joita on yhteensä 21 kategoriaa ja yli 100 alakategoriaa. (Framework for Improving… 2018, 6–8, 13.)

Kansallinen turvallisuusauditointikriteeristö Katakri on Suomen viranomaisen käyttämä työkalu organisaatioiden auditoimiseen, joka auttaa viranomaista esimerkiksi arvioimaan, miten hyvin yritykset kykenevät suojaamaan viranomaisen salassa pidettävää tietoa sekä miten he kykenevät yhteistyöhön julkisen hallinnon kanssa. Myös yritykset voivat käyttää työkalua suojaustasonsa määrittämiseen ja mittaamaan sen kykyä suojata turvallisuusluokiteltua aineistoa. Katakri ei niinkään aseta ehdottomia vaatimuksia tietoturvallisuudelle, vaan enemmänkin pyrkii valvomaan lainsäädännän vaatimusten sekä kansainvälisten tietoturvatavoitteiden toteutumista. Katakri muodostuu kolmesta eri osa-alueesta, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Jokaiselle osa-alueelle määritellään omat turvallisuusvaatimukset sekä annetaan esimerkkejä näiden vaatimusten toteuttamiseksi. Katakri-työkalua voidaan hyödyntää esimerkiksi organisaatioiden, viranomaisten tai yhteisöjen turvallisuustyön kehitykseen sekä kyberturvallisuuden arviointiin. (Katakri 2020 tietoturvallisuuden…, 5–6.)

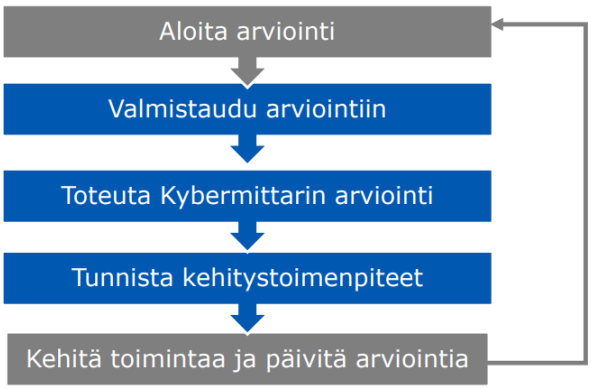
VAHTI-ohjeet ovat kansallinen julkaisusarja, joita julkaisee valtiovarainministeriön asettaman valtionhallinnon tietoturvallisuuden johtoryhmä. He luovat oheistuksia, määräyksiä ja vaatimuksia, joiden mukaan tietojärjestelmät ja prosessit tulee rakentaa, mikäli käsitellään valtionhallinnon tietoja. VAHTI:n tehtävänä on valtion- ja julkishallinnon tietoturvallisuuden sekä kyberturvallisuuden ohjaaminen, kehittäminen sekä koordinointi. He käsitelevät mm. tieto- ja kyberturvallisuuden linjauksia sekä toimenpiteisiin liittyviä ohjausasioita, ja tukee tietoturvallisuuteen liittyvässä päätöksenteossa ja valmisteluissa valtioneuvostoa ja valtionhallintoa. Ohjeistosta löytyy hyviä työkaluja ja ohjeita kaikille yrityksille kyberturvallisuuden

kehittämiseen, ja nämä löytyvät kaikki valtionvarainministeriön verkkosivuilta. (VAHTI 5/2013 Päätelaitteiden…2020.)

4.4 Kybermittari

Tässä opinnäytetyössä yhtenä nykytila-analyysin menetelmänä käytetään liikenne- ja viestintäministeriö Traficomin kyberturvallisuuskeskuksen (Kybermittari Kansallinen kyberturvallisuuden…2020, 3-4) kehittämää maksutonta ja kaikkien vapaasti saatavissa olevaa työkalua, jota voidaan käyttää yritysten kyberturvallisuuden arviointiin ja kehittämiseen. Kybermittarin avulla voidaan muodostaa kokonaisvaltainen kuva yrityksen kyberturvallisuuden nykytilasta sekä löytää mahdollisia kehityskohteita ja parantaa yritysten kykyä torjua kyberuhkia. Kybermittari on suunniteltu yritysten johdolle ja tietoturva-ammattilaisille, jotta sen avulla voitaisiin paremmin hallita, vertailla ja kehittää kyberturvallisuutta. Kybermittari kattaa myös kyberturvallisuuden tärkeimmät riskienhallinnan toimenpiteet, työkalun avulla saa luotua automaattiset raportit yrityksen kyberturvallisuuden kypsyystasosta. Raporteissa kybermittari esittää organisaation kyvykkyyden tason kyberriskien tunnistamisesta, suojautumisesta ja havainnoinnista sekä kyberriskeihin reagoinnista ja palautumisesta mahdollisen riskin toteutumisen jälkeen. Kybermittari on luotu myös mahdollistamaan yritysten ja toimialojen keskinäisen vertailemisen sekä parhaiden käytäntöjen jakamisen eteenpäin ja se auttaa tunnistamaan yrityksen ja koko yhteiskunnan kannalta kriittisimmät palvelut ja niiden riskit. Kybermittarin pohjan luo edellisessä luvussa esitetty kansainvälisesti tunnetut NIST kyberturvallisuus viitekehys sekä Cybersecurity Capability Maturity Model (C2M2).

Kybermittarin hyödyntämistä helpottamaan kyberturvallisuuskeskus on suunnitellut arviointiprosessin, joka suositellaan otettavaksi osaksi toiminnan jatkuvaa kehittämistä. Kuviosta 2. voidaan nähdä arviointiprosessin vaiheet. Viisivaiheinen arviointiprosessi muodostuu arvioinnin aloittamisesta, siihen valmistautumisesta, kybermittarin arvioinnin toteuttamisesta sekä kehitystoimenpiteiden tunnistamisesta ja toteuttamisesta ja jatkuvasta arvioinnista. (Kybermittari Kansallinen kyberturvallisuuden…2020, 5.)



Kuvio 2: Kybermittarin arviointiprosessi (Kybermittari -esittely 2020, 21)

Ensinäkin tulisi luoda johtoportaassa päätös arvioinnin toteuttamisesta ja miten se organisoidaan. Arviointiprosessin ensimmäisessä vaiheessa päätetään siis arvioinnin toteutuksesta, arvioinnin kohteesta sekä nimetään arvioinnille sponsori ja vetäjät. Tärkeä vaihe tässä kohtaa on osa-alueen valinta, kattaako arviointi koko organisaation toiminnan vai kohdistetaanko se kerralla vain yhteen kriittiseen palveluun. Jälkimmäistä suositellaan varsinkin isommissa organisaatioissa tai jos osa-alueen prosessit ja käytännöt eivät ole riittävän yhteneväisiä. Arviointiprosessin seuraavassa vaiheessa tulisi tarkemmin rajata arvioitavana oleva toiminnan osa-alue ja tunnistaa osa-alueen kriittiset riippuvuudet sekä tunnistaa arviointiin tarvittavat asiantuntijat ja sopia arviointitavasta ja arvioinnin aikataulusta. Osa-alueen rajaus suositellaan tekemään erityisen huolella, jotta arviointi voitaisiin toteuttaa tavoiteaikataulussa ja tuloksia voitaisiin tulkita myöhemmin oikein. Arviointitapana työpajamuotoinen tapa on todettu toimivaksi. Kolmannessa vaiheessa arvioinnin vetäjä, arvioinnin sponsori ja organisaation asiantuntijat suorittavat arvioinnin kybermittarin avulla. Tämän jälkeen prosessin neljännessä vaiheessa analysoidaan arvioinnista saadut tulokset ja määritetään organisaation toiminnalle tavoitetaso sekä tunnistetaan ja valitaan tärkeimmät kehitystoimenpiteet. Viimeisessä vaiheessa toteutetaan kehityssuunnitelman toimenpiteitä ja käynnistää tarvittaessa uusi arviointiprosessi, mikä olisi hyvä tehdä noin 1–2 vuoden välein. (Kybermittari kansallinen kyberturvallisuuden…2020, 6–7.)

Kybermittari antaa arvioinnista organisaation kyberturvallisuuden kypsyystason, minkä määrittämiseen käytetään neljää eri tasoa 0–3. Tämä perustuu organisaation kyberturvallisuuden kyvykkyyteen sekä ohjaa kehitystä kypsyystasolta toiselle. Arvioinnissa käydään läpi yksitoista eri kyberturvallisuuden osiota, jotka ovat nähtävissä kuviossa 3. Näille jokaiselle määritellään kypsyystaso. Jokainen osio pitää sisällään tyypillisiä hyväksi havaittuja kyberturvallisuuden tavoitteita sekä käytäntöjä, joita kybermittari myös arvioi. Käymällä kaikki osiot huolella läpi, saadaan hyvä kokonaiskuva yrityksen kyberturvallisuudesta ja löydetään mahdolliset heikkoudet ja kehityskohteet. (Kybermittari Kansallinen kyberturvallisuuden…2020, 10-11.)

CRITICAL – Kriittisten palveluiden suojaaminen
RISK - Riskienhallinta
DEPENDENCIES– Toimitusketjun ja ulkoisten riippuvuuksien hallinta
ASSET – Omaisuuden, muutoksen ja konfiguraation hallinta
ACCESS – Identiteetin- ja pääsynhallinta
THREAT – Uhkien ja haavoittuvuuksien hallinta
SITUATION - Tilannekuva
RESPONSE – Tapahtumien ja häiriötilanteiden hallinta
WORKFORCE – Henkilöstön hallinta
ARCHITECTURE - Kyberturvallisuusarkkitehtuuri
PROGRAM - Kyberturvallisuusohjelma

Kuvio 3: Kyberturvallisuuden osiot kybermittarissa (Kybermittari -esittely 2020, 41)

Organisaation kyberturvallisuuden kypsyystaso muodostuu toteutettujen käytäntöjen ja niiden vaativuuden mukaan, ja mitä vaativampia käytäntöjä yritys toteuttaa, sitä korkeampi on tämän osa-alueen kypsyystaso. Laskentaprosessi etenee niin, että aluksi kaikkien osioiden käytännöt arvioidaan joko toteutuneeksi tai ei toteutuneeksi, jonka jälkeen toteutuneiden käytäntöjen mukaan lasketaan jokaisen tavoitteen kypsyystaso prosenttiosuuksia hyödyntäen. Sitten vielä jokaisen osion kypsyystaso määritellään osion heikoimman tavoitteen mukaan asteikolla 0-3 niin, että jos jonkin tavoitteen kypsyystaso on 1, tulee koko osion kypsyystasoksi 1 heikoimman tavoitteen mukaan. Jotta voi saavuttaa tietyn kypsyystason, tulee joko kaikkien tai yli puolien kyseisen kypsyystason käytännöistä toteutua eikä seuraavalle kypsyystasolle voi päästä ennen kuin kaikki alempien kypsyystasojen käytänteet on toteutuneet. (Kybermittari kansallinen kyberturvallisuuden…2020, 11-13.)

5 Kohti parempaa kyberturvallisuutta

5.1 Yrityksen nykytilan selvittäminen

Jotta voidaan parantaa yrityksen kyberturvallisuutta, tulee yrityksen lähtötilanne ja koko toimintaympäristö määritellä tarkasti, jotta tiedetään mitä suojaustoimenpiteitä yrityksessä on jo olemassa ja mitä he tarvitsevat, mikä sitä uhkaa ja mitä kaikkea vastaan yritys taistelee. Yrityksen tulee ymmärtää, mitkä tietoteknisen ympäristön osat ovat tärkeimpiä sen liiketoimintatavoitteiden saavuttamiseksi. Määrittelyssä tutkitaan yrityksen koko teknisen liiketoimintaympäristön osat. Toimintaympäristöä määriteltäessä selvitetään mitä järjestelmiä yrityksen eri verkoissa on ja mitkä järjestelmät ovat yhteyksissä toisiinsa, kenellä on pääsy mihinkin tietoon ja kuka omistaa minkäkin verkon tai palvelun. Mikäli yritykselle on tärkeää esimerkiksi pitkäkestoiset asiakassuhteet, on hyvä varmistaa, asiakastietojen suojaus, tilaustoimitusjärjestelmän häiriötön toimivuus sekä organisaation internetsivujen jatkuva toimivuus. Koko ympäristön täydellinen ymmärtäminen voi olla haasteellista varsinkin, jos verkot ja järjestelmät ovat kasvaneet ja laajentuneet ajan saatossa. (Kyberturvallisuus ja yrityksen…2020, 11.)

Koko toimintaympäristön määrittäminen on tärkeää, koska yritys voi joutua hyökkäyksen kohteeksi myös esimerkiksi alihankkijoiden, kumppaneiden tai asiakkaidensa kautta tai myös täysin sivullisena uhrina esimerkiksi haittaohjelmatartunnan kautta, joten myös palveluntarjoajien ja kumppaneiden kanssa jaettavat tiedot ja järjestelmät tulee muistaa tarkistaa. (Kyberturvallisuuden vahvistaminen suomalaisissa… 2022, 2-3.) Kumppanit ja muut yritykset ovat monesti myös hyviä tietolähteitä, ja heiltä voi saada neuvoja erilaisista uhista ja hyviksi havaituista suojaustoimenpiteistä. Jaettu tieto on kaikkien parhaaksi ja hyödyksi, joten

yhteistyösuhteiden ja tiedonvaihdon kehittäminen on kannattavaa kyberuhilta suojautumisessa. (Kyberturvallisuus ja yrityksen…2020, 18.)

Eli aluksi tärkeää on määritellä yrityksen lähtötila sekä ne yrityksen tietotekniset osat, jotka ovat kriittisiä liiketoiminnan tavoitteiden saavuttamiseksi ja varmistetaan, että erityisesti näitä toimintoja suojataan. Tärkeät liiketoimintatekijät voivat olla sellaisia, joita ilman yritys ei pysty toimimaan tai niiden vahingoittuminen voisi uhata yrityksen mainetta tai aiheuttaa taloudellista tappiota esimerkiksi henkilötiedot, immateriaalioikeudet, verkkosivustot, teollisuuden ohjausjärjestelmät. (Kyberturvallisuus ja yrityksen…2020, 10.)

Yrityksien ongelmana on usein se, ettei heillä ole kokonaisymmärrystä siitä mitä kaikkea heidän kyberympäristöönsä kuuluu ja mitä siellä tapahtuu. Kattava tilannekuva onkin ensiarvoisen tärkeä yrityksen kyberturvallisuuden ja kyberriskien hallitsemiseen. Tilannekuva kertoo kyberturvallisuuden nykytilan ja sen missä tällä hetkellä mennään kyberturvallisuuden suhteen. Tilannekuvan luominen aloitetaan inventoimalla kaikki yrityksen järjestelmät ja niiden kytkökset toisiinsa sekä yrityksen sisällä eri osastojen välillä että yrityksen ulkopuoliset kytkökset yhteistyökumppaneihin ja yhteiskunnan infrastruktuuriin. Tilannekuvan luomisessa ei pidä kuitenkaan keskittyä pelkästään tekniseen kuvaan vaan ottaa huomioon myös liiketoimintanäkökulma ja pohtia mitkä järjestelmät ovat yrityksen liiketoiminnan kannalta tärkeimpiä. (Limnéll ym. 2014, 189-191.)

5.2 Kyberturvallisuuden johtaminen

Digitaalisessa nyky-yhteiskunnassa yritykset ovat entistä riippuvaisempia erilaisista digitaalisista palveluista ja järjestelmistä, ja tätä kautta myös altistuu koko ajan uudenlaisille riskeille. Kyberturvallisuuteen pitäisi yrityksissä suhtautua vakavasti, ja on tärkeää, että yritysjohdolla ja hallituksella on riittävät taidot myös kyberturvallisuudesta, jotta he voivat turvata yrityksen toimintakyvyn myös kyberuhkien varalta. (Kyberturvallisuus ja yrityksen…2020, 3.) Ylimmän johdon osallistuminen ja sitouttaminen on elintärkeässä roolissa, jotta yrityksessä päästään kohti parempaa kyberturvallisuutta. Johdon tulee ensiksi ymmärtää kyberturvallisuuden merkitys, näyttää esimerkkiä ja lisätä tämä omalle asialistalleen sekä päätöksentekoprosesseihin, jotta kyberturvallisuutta voidaan kehittää koko organisaatiossa. (Merenkulun kyberturvallisuus – varustamojen 2021, 7.)

Kyky torjua uudenlaisia uhkia vaatii hyvää johtamista, ja että kyberturvallisuutta ylipäätänsä edes johdetaan yrityksessä. Ei ole ennen kuulumatonta, että yrityksessä ei olisi vielä ollenkaan keskitytty kyberturvallisuuden kehittämiseen tai sitten vastuu tästä on määrätty vain yhdelle henkilölle tai tiimille, mutta johto ei ole sen enempää ollut kiinnostunut tai seurannut kyberturvallisuutta. Varisinkaan jos mitään ei ole sattunut, voidaan helposti ajatella, että on varauduttu riittävän hyvin. (Kärkkäinen 2020.) Uskon myös, että monessa yrityksessä voidaan ajatella, että ei mitään satu, kun ei ole ennenkään sattunut ja monesti reagoidaan vasta

sitten kun jotain oikeasti sattuu tai sitten ajatellaan, että kyllä joku muu hoitaa. Jo sillä, että tiedostetaan asian tärkeys ja otetaan vähän asioista selvää ja ollaan kiinnostuneita, voidaan esimerkiksi tietomurron riskiä pienentää merkittävästi (Kärkkäinen 2020). Mikäli kyberturvallisuutta ei ole aiemmin huomioitu yrityksessä, tulisi se tehdä viimeistään nyt. Kyberturvallisuus on johdon vastuulla ja sen tehtävänä on varmistaa riittävät resurssit turvallisuuden varmistamiseksi ja mahdollisten toimenpiteiden suorittamiseksi. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022.)

Kyberturvallisuuden johtamisessa tulisi miettiä paljon siihen ollaan valmiita käyttämään resursseja ja miten kyberturvallisuus nähdään yrityksessä. Onko se esimerkiksi budjettilähtöistä tai siihen varautuminen vain teknisten välineiden ostamista vai kenties koko yrityksen liiketoiminnan kannalta keskeinen menestystekijä. Kun kyberturvallisuutta johdetaan hyvin, varaudutaan yllättäviin tilanteisiin ja tapahtumiin jo etukäteen ja mietitään toimintatapoja, mikäli kyberuhka toteutuu sekä pyritään pienentämään kyberuhkiin liittyviä riskejä. (Kärkkäinen 2020.) Ennaltaehkäisy onkin tärkeä tekijä kyberturvallisuuden johtamisessa. Yrityksen tulisi pystyä ennalta löytämään ja reagoimaan kyberturvallisuusuhkiin oikealla tavalla. Tavoitteena on, että yritys olisi hyökkääjän silmissä kannattamaton kohde, johon hyökkäys olisi hankalaa. (Pienyritysten kyberturvallisuusopas 2020, 13.) Johdon tulee myös selvästi määritellä ja päättää mitä riskejä yrityksessä hallitaan ja mitä vastaan pyritään suojautumaan sekä mitä riskejä se taas on valmis sietämään. Esimerkiksi yritys voi päättää hyväksyä sen riskin, ettei sähköposti hetkeen toimi, mutta henkilötietoja ei saa päätyä julkisuuteen hetkeksikään. Kyberturvallisuus on jatkuvaa toimintaa ja onkin tärkeää myös jatkuvasti seurata toimenpiteitä. Yrityksen tulee tarkistaa ja arvioida säännöllisesti toimintaansa sekä muuttaa ja reagoida, mikäli ilmenee uusia uhkia. (Kyberturvallisuus ja yrityksen…2020, 14-15.)

Kyberturvallisuuden tulisi olla yrityksessä strategisen tason asia, jolla on selkeä strateginen tavoitetila, jota kohti pyritään ja tehdään sen eteen vaadittuja toimenpiteitä. Myös kyberturvallisuus tulee ajatella jatkuvana prosessina, jota tulee suunnitella ja johtaa kohti päämääriä. (Limnéll ym. 2014, 42-43.) Johdon tulee lisäksi varmistaa, että kyberturvallisuus on linjassa yrityksen muun strategian kanssa ja myös kyberriskien tulee olla osa yrityksen päivittäistä riskienhallintaa ja päätöksentekoa. (Kyberturvallisuus ja yrityksen…2020, 22-23.) On tärkeää, että yritys tuntee kybermaailman ja ymmärtää ja tunnistaa yrityksen kaikki eri tietotekniset ketjut ja linkitykset. Esimerkiksi tuotantoa, jakelua, taloutta, myyntiä sekä markkinointia kaikkia hallitaan nykyään lähes kokonaan kyberavaruudessa. Monissa yrityksissä edelleen vanhanaikaisesti jaotellaan tieto- ja kyberturva IT-osaston vastuulle tai kokonaan vain muutaman henkilön osaamisen varaan. Bittien maailma läpäisee kuitenkin kaikki yrityksen tärkeät toiminnot, joten kyberturvallisuus tulee olla osa koko liiketoimintaa ja strategiaa. Kyberturvallisuus ja teknologia usein unohdetaan, sillä niiden olemassaolo monesti havaitaan vasta kun on liian myöhäistä silloin, kun kaikki ei enää toimi oletetusti. (Limnéll ym. 2014, 56-57.)

5.3 Kyberhyökkäyksiltä suojautuminen

On olemassa yrityksiä, joiden järjestelmiin on jo hyökätty sekä yrityksiä, jotka eivät vain tiedä sitä vielä, sillä lähes kaikissa verkoissa ja järjestelmissä on käynyt tunkeilijoita, ja lähes kaikkiin isoimpien yritysten tietoverkkoihin on tunkeuduttu ympäri maailman. (Limnéll ym. 2014, 82.) Kyberhäiriöt ovat yleisiä digitaalisessa yhteiskunnassa, ja viime aikojen näkyvät kyberturvallisuusloukkaukset ovat saaneet kaikki kiinnittämään taas enemmän huomiota kyberturvallisuusuhkiin ja niiltä suojautumiseen. (Kärkkäinen 2020). Tänäänkin yli miljoona ihmistä maailmanlaajuisesti joutuu kyberrikoksen uhriksi. (Williams 2012, 14). Kuten aiemmin esitettiin, yleisempiä kyberhyökkäyksien keinoja ovat tietojenkalastelu, haittaohjelmat sekä palvelunestohyökkäykset. Kyberhyökkääjät toimivat niin, että he yrittävät löytää yrityksen toiminnan kannalta merkitykselliset digitaaliset palvelut ja löytämään pääsyn niihin sekä etsimään yrityksen järjestelmistä tietoturva-aukkoja ja hyödyntämään niitä. Hyökkääjät monesti hyödyntävät aivan perinteisiä julkisesti saatavalla olevia sovelluksia ja tapoja. Monesti hyökkääjät onnistuvat juurikin hyödyntämään organisaatioiden perustason tietoturvapuutteita, ja monet hyökkäykset olisivat estettävissä huolehtimalla kyberturvallisuuden perustason asiat kuntoon. Hyökkäyksiä pystytään torjumaan huolellisella tietoturvatyöllä, jonka tulee olla kunnossa sekä omissa että myös kumppaneiden digitaalisissa palveluissa. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022, 3 & Kyberturvallisuus ja yrityksen… 2020, 28.)

Kyberuhkia varten on tärkeä varautua ja niiden ikäviltä vaikutuksilta suojautua. Täydellistä kyberturvallisuutta ei kannata suunnitella, sillä sitä ei ole olemassa ja lisäksi on tärkeä pitää mielessä, että kybermaailma muuttuu ja kehittyy koko ajan. Kyberturvallisuuden perusasiat tulisi olla kunnossa jokaisessa yrityksessä, jotta pystytään suojautua yllätyksien varalta ja turvata toiminnan jatkuminen kyberhyökkäyksen aikana sekä palauttaa normaali tila mahdollisimman nopeasti hyökkäyksen jälkeen. Eli tärkeää on pistää yrityksessä perusasiat kuntoon, lisätä yleisesti kaikkien tietoisuutta ja toimintakykyä sekä pitää tietoturva ajan tasalla. Kyberhyökkäyksien torjunnassa tärkeässä roolissa on myös hyökkäysten esiin tuominen, kun kyberhyökkäyksistä raportoidaan ja tietoja kerätään ja jaetaan julkisesti eteenpäin, saadaan lisää arvokasta tietoa, jonka avulla voidaan varautua paremmin. (Limnéll ym. 2014, 106-107.) Suuri osa kyberhyökkäyksistä toteutetaan hyvin yksinkertaisilla välineillä, kuten huijaussähköposteilla, joiden avulla yritetään kerätä esimerkiksi käyttäjätunnuksia ja salasanoja. Kyberturvallisuutta voidaan myös parantaa hyvin yksinkertaisillakin keinoilla, kuten kouluttamalla henkilöstöä tunnistamaan näitä huijausyrityksiä (Kyberturvallisuus ja yrityksen…2020, 8.)

Kyberturvallisuuden hyvä perustaso voidaan määritellä esimerkiksi ISO/IEC 27000 -tietoturvastandardin ja NIST:n kyberturvallisuuskehyksen avulla. Kyberturvallisuuskeskuksen kybermittari auttaa myös arvioimaan yrityksen kyberturvallisuuden tilaa. Eri toimenpiteet tulee räätälöidä yrityksen merkittävimpien riskien mukaan, jolloin näillä perustason toimenpiteillä

pystyy estämään yleisimpiä kyberhyökkäyksiä. (Kyberturvallisuus ja yrityksen…2020, 28.) Konkreettisia tärkeitä perustason toimenpiteitä, jotka vähintään tulisi yrityksessä olla kunnossa suojautuakseen kyberhyökkäyksiltä on monivaiheinen tunnistautuminen, tietoturvapäivityksien asennus, tietoliikenteen turvallisuuden varmistaminen, haittaohjelmilta suojautuminen, palvelunestohyökkäyksiin varautuminen, pilvipalveluiden suojaus, etäyhteyksien turvallisuus, varmuuskopiot sekä langattomien yhteyksien tarkastelu. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022.)

Monivaiheinen tunnistautuminen on turvallisuustoimenpide, jonka mukaan järjestelmiin kirjautumiseen vaaditaan useampi tunnistautumistapa, esim. salasana, puhelimeen lähetettävä koodi sekä sormenjälki. Jo kaksivaiheinen tunnistautuminen vähentää selvästi hyökkääjän mahdollisuuksia tietojenkalasteluun. Tärkeä suojautumiskeino on lisäksi se, että kaikki uudet tietoturvapäivitykset asennetaan aina viipymättä ja käyttöjärjestelmien ja ohjelmistojen automaattiset päivitykset on otettu käyttöön, sillä päivittämättömistä järjestelmistä rikolliset osaavat nopeasti löytää ja hyödyntää turvallisuuspuutteita. Lisäksi on tärkeää tehdä säännöllisesti varmuuskopiot tiedostoille ja säilyttää nämä eri paikassa kuin omaan tietokoneeseen yhdistetyllä laitteella. Varmuuskopioinninkin on hyvä olla automatisoitua. Yritys voi esimerkiksi joutua tuhohyökkäyksen kohteeksi, jossa kaikki tiedot tuhotaan, jolloin ainoa keino selvitä tästä ovat ajantasaiset ja palautettavat varmuuskopiot. (Pienyritysten kyberturvallisuusopas 2020, 11-12.) Tietoliikenteen turvallisuutta voidaan parantaa estämällä tietoliikenneverkkojen palomuureilla kaikki yritykselle tarpeeton tietoliikenne, niin saapuva kuin ulospäin lähtevä tietoliikenne. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022, 4.)

Kohti parempaa kybersuojautumista päästään myös oikeanlaisella käyttöoikeuksien hallinnalla, jossa mietitään, kenellä on oikeus päästä mihinkin tietoon yrityksessä käsiksi ja rajataan käyttöoikeuksia niiltä kenellä ei ole tarvetta tietyn laiseen tietoon. Pääkäyttäjätunnuksia ja järjestelmänvalvojan oikeuksia rajataan myös, sillä näitä ei tarvita normaalikäytössä. Mikäli rikollinen onnistuu tunnusten kalastelussa, auttaa rajatut käyttöoikeudet suojaamaan osaa tiesoista. Jokaisella tullisi olla myös omat tunnukset eikä yhteisiä tunnuksia saisi käyttää. Salasanan sijasta suositellaan sanalausetta, joka on vaikeampi murtaa. (Pienyritysten kyberturvallisuusopas 2020, 14-15.)

Myös työntekijöillä on tärkeä rooli tietoturvassa ja hyökkäyksien torjumisessa. Jotta työntekijät osaavat tunnistaa esimerkiksi epäilyttäviä sähköposteja tai linkkejä, tulee henkilöstön tietoisuutta jatkuvasti lisätä ja järjestää tietoturvakoulutusta. (Pienyritysten kyberturvallisuusopas 2020, 13.) Tietoturvauhkien nopea kehittyminen ja niiden merkityksellisemmät vaikutukset vaativat koko ajan entistä parempaa kykyä puolustautua niitä vastaan. Perustason toimenpiteet eivät tässä vaiheessa aina enää riitä, vaan tarvitaan kehittyneempiä tietoturvaratkaisuja, mutta tässä opinnäytetyössä keskitytään pienyrityksen kannalta keskeisiin perustason toimenpiteisiin.

5.4 Kyberriskienhallinta

Kyberriskienhallinnalla tarkoitetaan niitä toimenpiteitä, joiden avulla voidaan tunnistaa, arvioida, seurata ja hallita kyberriskejä. Tällaisia toimenpiteitä voivat olla esimeriksi riskin hyväksyminen, välttäminen, pienentäminen tai siirtäminen. (Kybermittari arviointityökalu 2022.) Koska kyberturvallisuuden kokonaisuus rakentuu ihmisistä, prosesseista ja teknologiasta, jää suojaukseen väistämättä aina aukkoja eikä täydellistä suojaa pysty rakentamaan, mutta oikeanlaisilla toimilla uhkien toteutumisen todennäköisyyttä ja niiden vaikutusta voidaan pienentää. (Kärkkäinen 2020.) Kyberturvallisuus onkin käytännön tasolla riskienhallintaa. Kyberriskienhallinta käynnistyy uhkien tunnistamisella ja niiden vaikutuksien analysoimisella ja selvittämällä niiden merkityksiä omaan toimintaa. Sen jälkeen uhkiin varaudutaan tarpeen mukaan ja jatkuvasti suunnitellaan sekä harjoitellaan kuinka toimia, jos jokin uhka toteutuisi. (VTT 2022.)

Jotta riskejä voidaan seurata johdonmukaisesti tulisi riskejä luokitella, jossa taas auttaa riskirekisterin ylläpitäminen, johon listataan kaikki yrityksen tunnistamat riskit. (Kybermittari arviointityökalu 2022.) Mikäli kyberriskejä luokitellaan vain ”tietoteknisiksi riskeiksi” on niiden tunnistaminen vaikeaa. Kyberriskeihin tulisikin soveltaa aivan samoja riskienhallinnan periaatteita kuin muihinkin riskeihin ja kyberriskien tulisi olla vahvasti osa organisaation muuta riskienhallintaa. Kyberriskejä olisi kuitenkin hyvä arvioida jopa useammin kuin muita riskejä, sillä kyberturvallisuuden ratkaisut ja teknologiat kehittyvät niin nopeasti. Eli organisaatioissa tarvitaan tietoinen päätös, miltä uhilta se aikoo suojautua, jottei toiminta ole tehotonta ja yritetä suojautua kaikelta. Aluksi tulisi kartoittaa eri riskitekijät ja määritellään näiden riskien mahdolliset vaikutukset ja todennäköisyydet jonka jälkeen voidaan määritellä tarkemmin, millaisia riskejä organisaatio on valmis sietämään ja millaisia riskejä se taas yrittää aktiivisesti hallita ja välttää. (Kyberturvallisuus ja yrityksen…2020, 15-20.)

Riskien hallinnan tulisi olla osa strategiaa ja kyberturvallisuusstrategiassa määritellä esimerkiksi yrityksen riskinottohalukkuus, riskien arviointikriteerit ja kuinka riskejä ylipäätänsä hallitaan (Kybermittari arviointityökalu 2022). Riskienhallinnan tulisi olla jatkuvan ajattelun- ja toimintatapojen luomisprosessi, jossa tavoitellaan riskien välttämistä, niiden vaikutusten minimoimista tai niiden kanssa elämään oppimista (Limnéll ym. 2014, 109). Yrityksellä täytyy myös olla valmiina suunnitelma, kuinka toimia uhan toteutuessa sekä kyky reagoida välittömästi mahdollisiin kyberhäiriöihin. Näitä tilanteita varten tulee olla selkeät nimetyt henkilöt, roolit ja vastuut sekä suunnitelma, kuinka toiminnan jatkuvuus turvataan ja toiminta palautetaan normaaliksi mahdollisimman pian. Lisäksi näitä tilanteita varten tulee jatkuvasti harjoitella ja suunnitelmia jatkuvasti päivittää. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022, 10.)

Henkilökunta & koulutus

Jopa 95 % yrityksiin kohdistuvista kyberhyökkäyksistä johtuu inhimillisestä virheestä (Cybernews 2022). Sanotaankin, että yrityksen heikoin lenkki ovat sen työntekijät, ja suurin uhkatekijä heidän aiheuttamansa inhimilliset erehdykset. (AIG 2022). Kyberturvallisuudessa täytyykin aina ottaa huomioon myös inhimillinen tekijä. Vaikka tietoturvaohjeet- ja käytännöt olisivatkin selkeät yrityksessä, niin ihmiset monesti silti saattavat toimia ajattelemattomasti, huolimattomasti, piittaamattomasti tai ymmärtämättömyydessä. Yritykselle voi olla merkittävä riski, mikäli sen henkilökunta ei osaa olla valppaana ja hallita kyberturvallisuuden perusasioita. (Limnéll ym. 2014, 46.)

5.5

Työntekijöiden koulutukseen ja osaamiseen panostaminen ovat siis selvästi tärkeä osa kyberturvallisuutta. Organisaation koko henkilöstöllä on tärkeä rooli sen kyberturvallisuuden varmistamisessa ja johdolla taas sen varmistamisessa, että sen henkilöstö on tarpeeksi tietoinen kyberturvallisuuden merkityksestä organisaation toiminnalle. Johdon tulee tukea koulutuksen ja viestinnän keinoin henkilöstön kyberosaamista ja lisätä tietoisuutta jatkuvasti. Henkilöstölle tulee säännöllisesti esimerkiksi järjestää työtehtävien kannalta riittävää tietoturvakoulutusta, jotta he osaavat huomioida työssään yleisimmät tietoturvauhat. Henkilöstölle tulee myös tiedottaa, minne heidän tulee ilmoittaa, jos he havaitsevat tietoturvapoikkeamia tai epäilevät niitä. (Kyberturvallisuuden vahvistaminen suomalaisissa…2022, 10-11.)

Yrityksen tulisi kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista – ja valmiutta sekä määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa organisaation kyberturvallisuuskulttuurin luomiseksi ja sopivan ja osaavan henkilökunnan takaamiseksi. Kyberturvallisuuteen liittyvistä ajankohtaisista asioista on hyvä säännöllisesti tiedottaa henkilökuntaa ja puhua kyberturvallisuusasioista avoimesti. Kyberturvallisuuteen liittyvät vastuut ja roolit tulee nimetä ja jakaa selkeästi sekä varmistaa ettei vastuut rajoitu pelkästään vain perinteisiin IT-rooleihin. Mahdollisten osaamispuutteiden vuoksi voidaan tarvita uusien työntekijöiden rekrytointia. Henkilöstön hallinnointiin kyberturvallisuuden näkökulmasta voivat kuulua lisäksi henkilökunnan turvallisuus- ja taustakartoitukset. (Kybermittari arviointityökalu 2022.)

Kyberturvallisuutta voi parantaa luomalla kyberturvallisuuden kulttuuria yritykseen ja ottamalla asiat osaksi keskustelua sekä lisäämällä työntekijöiden tietoisuutta kyberriskeistä. (Kyberturvallisuus ja yrityksen…2020, 24.) Johdon on hyvä rakentaa yritykseen positiivista kyberturvallisuuskulttuuria, missä kyberturvallisuus olisi perustaito, johon tietoisesti panostetaan ja jota jatkuvasti kehitetään. Avoimuus ja asioista puhuminen lisää tietoisuutta ja kun opittu jalostetaan osaksi kyberturvallisuuskulttuuria, ollaan askel edellä parempaan. (Limnéll ym. 2014, 38-39.)

5.6 Kyberturvallisuussuunnitelma

Jokaisella yrityksellä tulisi olla jonkinnäköinen kyberturvallisuussuunnitelma, jotta voidaan varmistaa, että kaikki yrityksessä tietävät miten kyberuhkia ehkäistään ja miten toimitaan, jos uhka toteutuu. Kyberturvallisuussuunnitelman tekeminen auttaa yritystä suuntaamaan ajatukset kyberturvallisuuteen. Kybertoimintasuunnitelmassa käsitellään erilaisten kyberratkaisujen lisäksi myös ennaltaehkäiseviä toimenpiteitä ja siinä voidaan käsitellä myös esimerkiksi jatkuvuuteen ja ennalleen palautumiseen liittyviä toimia. Mitä kattavampi suunnitelma on tietojen, verkkojen ja laitteiden suojaamiseksi, sitä paremmin yllätyksiltä vältytään. Kyberturvallisuussuunnitelman olisi hyvä pitää sisällään ainakin seuraavat neljä osa-aluetta:

- Määräysten noudattaminen: Tarkat ohjeet, kuinka yrityksessä käsitellään tietoja ja miten esimerkiksi EU:n tietosuoja-asetusta noudatetaan.
- Infrastruktuurin suojaaminen: Suojaussuunnitelma siitä, kuinka tietoja turvataan ja miten ohjelmisto- ja tietoturvapäivitykset hoidetaan ja miten tiedot varmuuskopioidaan ja kuka näistä vastaa. Suunnitelmaan tulee sisällyttää johdonmukainen monitasoinen ohjelmistosuojaus kuten virustorjunta, palomuurit, haittaohjelmien torjunta ja hyökkäyssuojaus sekä kattava vakuutusturva.
- Palautuminen ennalleen: Toimintasuunnitelma siitä, miten toimitaan tietomurron sattuessa, miten tietomurto eristetään sekä liiketoiminta palautetaan ennalleen mahdollisimman nopeasti. Lisäksi tulee kirjata, kuka vastaa viestinnästä viranomaisten, asiakkaiden, kumppanien ja alihankkijoiden suuntaan ja hoitaa vakuutuskorvausten hakemisen tällaisissa tapauksissa.
- Kouluttaminen: Viestintästrategian luominen koko yrityksen henkilöstölle internetin ja sähköpostin käytöstä ja parhaista käytännöistä, mikä pitää sisällään selkeät ohjeet näiden hyväksyttävästä käytöstä, huijausten havaitsemisesta, yritysverkon etäkäytöstä, sosiaalisen median säännöistä, salasanojen hallintajärjestelmistä sekä tapahtumien raportoinnista. (AIG 2022.)

Limnéllin ym. (2014, 180, 189-196) mukaan kyberturvallisuussuunnitelman tulee sisältää kyberriskien pienentämiseen ja sietokyvyn kasvattamiseen tähtääviä operatiivisia suunnitelmia ja projekteja, jotka voidaan jakaa kolmeen pääluokkaan:

- Ajantasainen tilannetietoisuus: Luodaan tilannekuva yrityksen koko kybertoimintaympäristöstä, kaikista yrityksen laitteista ja järjestelmistä ja niiden kytköksistä toisiinsa sekä yrityksen ulkopuolelle. Mukaan otetaan myös liiketoimintanäkökulma, ja mietitään mitkä ovat liiketoiminnan kannalta tärkeimmät järjestelmät. Tilannekuva tulee pitää ajan tasalla, jotta voidaan reagoida nopeasti muuttuvaan kyberympäristöön riittävän hyvin. Tilanne kuva kertoo sen hetken kybertoimintaympäristön tilan ja reagoi poikkeamiin.

- Tehokas kyberturvallisuus johtaminen ja kyberturvallisuusoperaatiot: Pitää sisällään tehokkaan tietoturvan hallinnan, kerroksittaisen suojautumisen, perusrutiinien automatisoinnin, 24/7 käytettävyyden ja -hallinnan sekä keskitetyn hallinnan.
- Dynaaminen turvallisuuden tuottaminen ja pelotevaikutus: Tarkoittaa nopeaa reagointia ongelmatilanteissa sekä ongelmien ennaltaehkäisyä ja aktiivisia vastatoimia. Esimerkki automaattisesta dynaamisesta vastatoimenpiteestä on palomuuri, joka reagoi automaattisesti tunkeutumisyritykseen ja estää sen.

6 Kehittämismenetelmät ja aineiston analyysi

6.1 Tutkimuksellinen kehittämistyö

Tämä opinnäytetyö toteutetaan tutkimuksellisena kehittämistyönä. Tutkimuksellisessa kehittämistyössä tutkimus ja kehittäminen liittyvät vahvasti yhteen. Tutkimuksellinen kehittämistyö saa usein alkunsa yrityksen tarpeesta kehittyä tai muuttua, ja sen tarkoituksena onkin ratkaista käytännön ongelmia, uudistaa vanhoja toimintamalleja sekä tuottaa uusia ideoita ja käytäntöjä. Tarkoituksena on siis kehittää entistä parempia ratkaisuehdotuksia sekä viedä niitä käytännössä eteenpäin. Työn etenemistä ohjaa käytännöstä esiin nousevat tavoitteet, jotka taas nojaavat teoriaan. Tutkimuksellisessa kehittämistyössä tärkeänä esiin nousee vuorovaikutuksellisuus, yhteistyö eri tahojen välillä, tutkiminen, kysymysten asettelu, tiedon tuottaminen, useiden erilaisten menetelmien käyttö, ohjaaminen ja ennakoimattomien tilanteiden kohtaaminen ja niihin reagoiminen. (Ojasalo, Moilanen & Ritakoski, 2015, 17-20.)

Tutkimuksellisen kehittämistyön etenemistä kuvataan monesti kuusivaiheisena prosessina, jotka ovat 1) kehittämiskohteen tunnistaminen ja alustavien tavoitteiden määrittäminen 2) kehittämiskohteeseen perehtyminen teoriassa ja käytännössä 3) kehittämistehtävän määrittäminen ja kehittämiskohteen rajaaminen 4) tietoperustan laatiminen sekä lähestymistavan ja menetelmien suunnittelu 5) kehittämishankkeen toteuttaminen ja julkistaminen eri muodoissa 6) kehittämisprosessin ja lopputulosten arviointi. Todellisuudessa prosessien ei tarvitse edetä järjestelmällisesti vaiheesta vaiheeseen vaan eri kohtiin voidaan palata edes ja takaisin. (Ojasalo ym. 2015, 23-24.)

Tutkimuksellinen kehittämistyö antaa omalle työlleni lähtökohdat, säännöt ja raamit, joiden mukaan työskentely etenee. Kehittämistyöni on saanut alkunsa kohdeyrityksen tarpeesta kehittää heikkoa kyberturvallisuuttaan, ja tämän kehittämistyön tarkoituksena onkin selvittää yrityksen kyberturvallisuuden lähtötaso ja antaa kehittämisehdotukset tämän parantamiseksi. Tutkimuksellinen kehittämistyö soveltuu tähän tarkoitukseen siis hyvin.

Lähestymistapana tapaustutkimus

Lähestymistavaksi tieteelliselle kehittämistyölleni valitsin tapaustutkimuksen (case study). Tapaustutkimuksessa perehdytään syvällisesti yhteen tapaukseen (case) ja tuotetaan sen kehittämiseksi tietoa tästä tietystä kohteesta. Tieteelliseen kehittämistyöhön tapaustutkimus soveltuu lähestymistavaksi hyvin silloin, kun halutaan ymmärtää syvällisesti jonkin yrityksen tilannetta ja tarkoituksena on ratkaista ilmenneitä ongelmia tai tuottaa tutkimuksen keinoin

6.2

kehittämisehdotuksia. Tapaustutkimuksessa ei välttämättä ole tarkoitus vielä viedä muutosta käytäntöön asti, vaan sen avulla luodaan kehittämisideoita ja ratkaisuehdotuksia. Tapaustutkimuksessa tarkoitus on tutkia syvällisesti kohdetta sen omassa ympäristössään. Tapaustutkimuksessa käytettäviä menetelmiä ovat esimerkiksi haastattelut, havainnointi, tilastot, asiakirja-aineistot, aikasarja-aineistot ja muut dokumentit kuten erilaiset esitteet, muistiinpanot, päiväkirjat ja kokouspöytäkirjat. Tapaustutkimus mahdollistaa monipuoliset menetelmävalinnat ja tähän voidaan käyttää sekä laadullisia että määrällisiä menetelmiä, kuten tässä tutkimuksellisessa kehittämistyössäni aion. (Ojasalo ym. 2015.)

Kvalitatiivinen eli laadullinen tutkimus on tutkimusmenetelmä, jossa tarkoituksena on ymmärtää, selittää ja tulkita tutkittavaa ilmiötä, ja tutkittavat aiheet ovat usein sellaisia, joita entuudestaan ei ole paljon tutkittu ja niitä pyritään ymmärtämään paremmin. Kvantitatiivinen eli määrällinen tutkimus taas pyrkii antamaan vastauksia kysymyksiin ”kuinka paljon tai kuinka usein”. Määrällisessä tutkimuksessa käytetään usein erilaisia mittareita, kuten kysely- tai haastattelulomaketta, ja mittarin avulla on tarkoitus saada määrällistä tietoa, joka esitetään numeerisessa muodossa. (Vilkka 2007, 12–16.)

Opinnäytetyössäni aion siis tapaustutkimusta hyödyntäen tuottaa kehittämisehdotuksia siihen, kuinka kohdeyrityksessä voitaisiin parantaa heidän kyberturvallisuuttaan. Case tässä tapauksessa on kohdeyrityksen kyberturvallisuuden nykytila, jota pyrin syvällisesti ymmärtämään ja selittämään sekä ehdottamaan ratkaisuja ilmenneisiin ongelmiin. Kyberturvallisuuden nykytilaa lähden selvittämään aluksi laadullisesti kattavalla puolistrukturoidulla yritysjohdon haastattelulla ja sitten määrällisesti kybermittari – työkalun testien avulla. Tämän jälkeen jatkan tulosten analysointia SWOT-analyysin avulla ja esitän kehittämisideoita ja ehdotuksia jatkotoimenpiteille. Tässä työssä tutkimusmenetelminä käytetään sekä kvalitatiivisia että kvantitatiivisia menetelmiä, sillä mielestäni näin saan tutkittavasta ilmiöstä monipuolisesti analysoitavaa aineistoa. Kyberturvallisuuden nykytilan selvittäminen kaipaa sekä laadullista kuvailevaa tietoa yritysjohdon näkemyksistä että määrällistä numeerista tietoa kybermittarista, joka tarjoaa näin hyvän mittarin tavoitteiden asettamiselle ja kehityksen seuraamiselle, kun tiedot ovat mitattavassa muodossa.

6.3 Puolistrukturoitu haastattelu yritysjohdolle

Kohdeyrityksen kyberturvallisuuden nykytilan selvittäminen aloitetaan puolistrukturoiduilla haastattelulla yritysjohdolle. Haastatteluilla on tarkoitus kartoittaa kyberturvallisuuden nykytilaa esimerkiksi johdon ja henkilökunnan kybertietämystä, mahdollisesti jo toteutuneita kyberuhkia, yleisempiä riskejä, nykyisiä käytäntöjä sekä kehityskohteita. Laadullisena tiedonkeruu menetelmänä puolistrukturoitu haastattelu sopii tähän tarkoitukseen hyvin, sillä se sopii aiheisiin, joita ei ole tutkittu vielä kovin paljoa, ja tilanteisiin, joissa haastateltavaa ei haluta ohjailla liikaa. Puolistrukturoitu teemahaastattelu on formaaliudessaan täysin strukturoidun lomakehaastattelun ja täysin avoimen haastattelun välimaastoa, ja on enemmänkin keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja. Puolistrukturoidussa haastattelussa seurataan ennalta määrättyä runkoa, mutta etukäteen suunnitelluista haastattelukysymyksistä saa myös poiketa tilanteen mukaan, ja voi kysyä kysymysten ulkopuolisiakin asioita. Kysymyksistä on tehty mahdollisimman avoimia ja sellaisia kysymyksiä, joihin on mahdollista vastata lyhyesti, vältetään, jotta haastateltavien omat ajatukset pääsisivät esiin ja haastateltava henkilö vastaisi kysymyksiin kuvailevasti ja mahdollisimman laajasti. Näin aineistosta saadaan riittävän laadukas. (Ojasalo ym. 2015, 41.)

Haastattelu toteutettiin kerralla yhtenä ryhmähaastatteluna, johon osallistui yrityksen kolme osakasta johtaja A, B ja C. Koska aihe ei ole yritykselle ennalta kovin tuttu, niin yhdessä haastateltavat pystyivät täydentämään toistensa vastauksia ja pohtimaan vastauksia yhdessä, mikä kenties jo opetti heille jotain aiheesta lisää tai sai kyseenalaistamaan asioita. Ryhmähaastatteluun päädyin myös, sillä tarkoituksena ei ollut saada selville yksilöiden henkilökohtaisia syvällisiä mielipiteitä vaan koko laajaa yrityksen kokonaiskuvaa. Haastattelu äänitettiin ja litteroitiin tarkasti jälkikäteen ja äänite poistettiin heti tämän jälkeen. Haastattelurungon olin suunnitellut jakamalla sen neljään teemaan: Yritysjohdon yleiskuva kyberturvallisuuden nykytilanteesta, kyberuhat ja niiden hallinta, tekniset lähtökohdat ja kyberturvallisuusosaaminen. Tarkemmat haastattelukysymykset löytyvät liitteestä 1.

Haastattelun ensimmäinen teema liittyi yritysjohdon yleiskuvan muodostamiseen heidän kyberturvallisuuden nykytilanteesta. Jo haastattelu vaiheessa selvisi hyvin pian, ettei yrityksen kyberturvallisuuden nykytila ole kovin vakuuttava ja kyberturvallisuudessa olisi paljon parantamisen varaa. Myös Yrityksen johto arvioi itse nykytilan heikoksi, sillä kyberturvallisuuteen ei ole vielä yrityksessä juurikaan panostettu. Johtaja C jopa totesi ettei usko, että tähän tarvitsisikaan kovin paljoa panostaa, koska ovat niin pieni ja ravintola- ja tapahtuma-alan yritys, että tarpeisiin nähden on jo riittävää. Johtaja A & B kuitenkin rupesivat listaamaan kehitettäviä asioita, joita pystyisi hyvin pienelläkin panostuksella laittamaan kuntoon ja näkivät myös kehittämisen tärkeäksi. He mainitsivat esimerkiksi heikot salasanat, joita helposti jaetaan kaikille tai kirjoitetaan ylös seinälle/vihkoihin ja joita vaihdetaan harvoin, vain jos jokin järjestelmä niin vaatii, ja että harvoja kansioita tai tiedostoja on salattu tarpeeksi, vaan niihin

pääse moni helposti käsiksi miltä vain koneelta. Hetki sitten oli myös selvinnyt, että johtaja A:n tietokone ei ollut yli vuoteen tehnyt ohjelmistopäivityksiä ja oli noin 7 vuotta vanha. Yleisesti he kokevat kuitenkin yrityksen ympäristön kyberturvalliseksi, vaikkakin joitain pieniä huijausyrityksiä on aika paljon viime aikoina ollut.

Tällä hetkellä yrityksen Kyberturvallisuus ja tietoturva on täysin ulkoistettu alan yritykselle, mutta kohdeyrityksellä ei ole tietoa sen tarkemmin, kuinka tätä hoidetaan eivätkä he ole keskustelleet aiheesta IT-kumppanin kanssa. Yrityksen johto kokee, että yrityksen ollessa vielä aika nuori ja kokoa ajan ollut paljon kehitettävää ja menty kovaa vauhtia, ettei aiemmin ole ollut aikaa ja resursseja kyberturvallisuudelle, mutta nyt voisi mahdollisesti enemmän olla. Johtaja A toteaa myös, että ehkä tähän mennessä on tehty liikaa ”hällä väliä asenteella” monia tietoturva asioita, että nyt voisi olla aika alkaa laittamaan perusasioita kuntoon. He voisivat olla valmiita laittamaan budjetista myös pienen osan kyberturvallisuuden parantamiseen, mutta hyvin pienen osan, ainakin aluksi.

Haastattelun toinen teema liittyi kyberuhkiin ja niiden hallintaan, josta selvisi, että yritykseen on kohdistunut jonkin verran häirintää ja huijausyrityksiä. Yritys on saanut tietojenkalasteluviestejä ja huijaussähköposteja, joissa on yritetty saada painamaan virheellistä linkkiä tai avaamaan sähköpostin liitetiedosto tai uhattu lunnaita vastaan. Yksi osakkaista oli saanut toimitusjohtajan nimissä valeviestin, jossa oli pyydetty maksamaan liitteenä oleva lasku nopeasti ja samoin yhtiökumppaniltaan valeviestin, jossa oli kysytty kuulumisia ja pyydetty tutustumaan oheiseen mielenkiintoiseen linkkiin. Yrityksen nimissä on myös sosiaaliseen mediaan luotu valetapahtumia sekä erilaisiin kilpailuihin käyty julistamassa virheellisesti voittajia ja pyydetty lunastamaan palkinto oheisen linkin kautta.

Keskeisimmiksi uhiksi yritysjohdon mielestä nousi esiin asiakastietojen leviäminen, yrityksen salaisten tietojen leviäminen ja tili/luottokorttitietojen leviäminen. Yritys kertoo käsittelevänsä paljon asiakastietoja ja erityisesti yritysasiakastietoja. Koska yritykseen on kohdistunut viime aikoina jonkin verran huijausyrityksiä, on uhkana myös, että joku kerta nämä onnistuu. Uhkaksi nousi esiin myös maineen menetys, mikäli yrityksen nimissä jatkuvasti luodaan valetapahtumia ja yritetään julistaa somekilpailuihin voittajia ja saada asiakkaita painamaan virheellisistä linkeistä. Yritys koki nykyisen maineensa kuitenkin niin hyväksi, ettei usko sitä ihan helposti menettävän. Yhdeksi uhkaksi johtaja A vielä mainitsi, että pelkästään sekin on jo iso uhka, että yrityksessä on niin vähän panostettu kyberturvallisuuteen ja osaaminen on heikkoa.

Yrityksessä tehdään jonkin verran etätöitä, mutta tämä ei ole kovin yleistä. Etätöihin liittyen ei ole havaittu tai tiedostettu mitään kyberturvallisuusuhkia. Yrityksen johto kyllä vie läppärin usein kotiin ja työskentelee myös kotoa käsin sekä käyttää samaa puhelinta työtehtäviin ja vapaa-ajalla ja puhelimelta pääsee sekä yrityksen että henkilökohtaiseen verkkopankkiin,

sähköpostiin ja Outlook:n kautta yrityksen tiedostoihin käsiksi. Yrityksen johto ei ole tarkkaan tietoinen mitä kyberturvallisuuteen liittyviä oikeudellisia vaatimuksia tai sopimusvelvoitteita heidän tulisi täyttää, päällimmäisenä kaikilla nousi esiin GDBR. Kyberturvallisuus ei ole osana yrityksen riskienhallintaa.

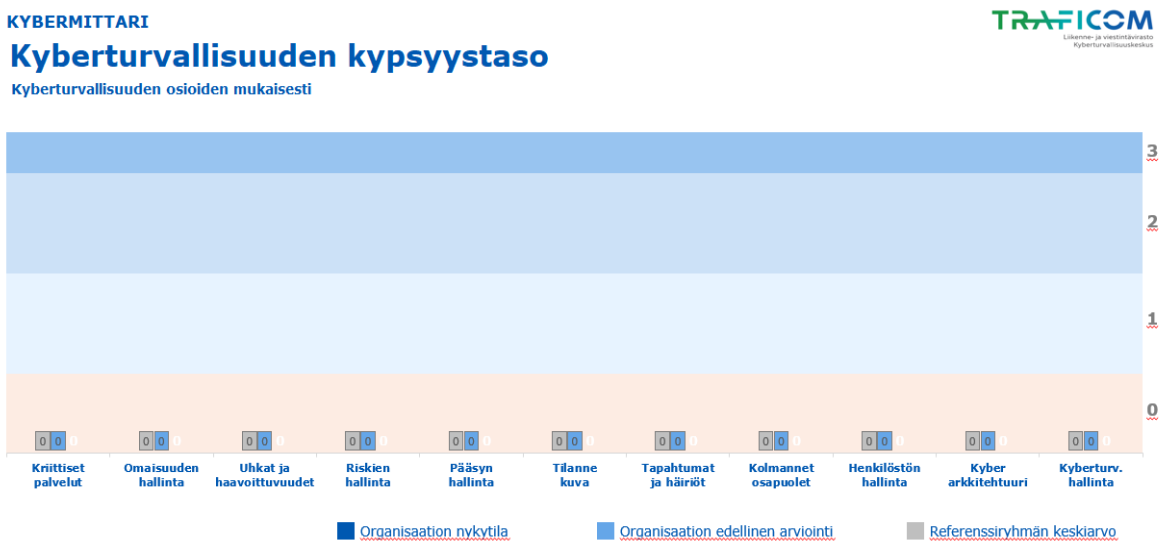
Kolmannessa haastattelun osassa selvitettiin teknisiä lähtökohtia. Yritys arvioi kriittisimmiksi tietoteknisiksi resursseikseen, joita ilman ei selviäisi Outlook sähköpostin, varauskalenterin sekä pilvipalvelun tiedostoille kuten tarjouspohjille, varausvahvistuksille ja asiakastiedoille. Myös Microsoft Word ja Excel koettiin tärkeiksi ja samoin internet, yrityksen verkkosivut, sosiaalisen median kanavat ja kassajärjestelmä. Konkreettisina käytäntöinä kyberturvallisuuden hallitsemiseen on lähinnä ollut vain ”jos on jokin ongelma, soita IT-firmaan”. Myöskään sen kummempia prosesseja tärkeiden järjestelmien, tietojen tai palvelujen tunnistamiseen tai näiden toimivuuden ja turvallisuuden seuraamiseen ei yrityksessä ole muuten, ellei IT-yrityksellä ole. Yrityksen johto ei myöskään ole tarkkaan tietoinen mitä järjestelmiä eri verkoissa on tai mitkä ovat yhteyksissä toisiinsa tai kenellä on pääsy mihinkin tietoon tai kuka omistaa minkäkin verkon ja palvelun. Kaikilta tietokoneilta pääsee käsiksi lähes kaikkiin tiedostoihin ja tietoihin. Turvallisuussyistä kassajärjestelmät ja maksuliikenne on tiedettävästi ainakin kytketty eri verkkoon kuin yrityksen koneet tai asiakkaillekin jaettava WIFI. Pääsy- ja käyttöoikeushallintaa eri laitteisiin ja järjestelmiin ei juurikaan pidetä yllä, vaan johto myöntää, että samoja tunnuksia saattavat käyttää usea henkilö eikä vanhoilta työntekijöiltä poisteta aina oikeuksia ja myös salasanoja kirjoitetaan monesti kaikkien nähtäville. Vaikka joihinkin järjestelmiin on erikseen pääkäyttäjätunnukset ja tunnuksia alemmilla oikeuksilla, saattavat monet käyttää näitä ainoita pääkäyttäjätunnuksia.

Viimeinen haastattelun teemaosuus oli kyberturvallisuusosaamisesta. Yrityksen johto kuvaa yhtenäisesti osaamisen heikoksi. Vastuuta kyberturvallisuudesta ei ole nimetty kellekään, vaan sitä hoitaa ainoastaan IT-yritys. Yrityksen johto kokee myös, ettei johto ja työntekijät ole tarpeeksi tietoisia mahdollisista kyberuhista eikä työn tekijöitä kouluteta tai tiedoteta kyberturvallisuuden osalta. Kyberturvallisuutta ei myöskään johdeta yrityksessä millään tasolla. Yrityksestä kyllä löytyy johdon koulutuksen kautta vahvaa osaamista riskienhallinnasta ja johtamisesta ja yleisesti yrityskulttuuri on jatkuvasti kehittämiseen ja uuden oppimiseen tähtäävä ja johtaminen ja vastuunjaot selkeää.

Kybermittari -työkalun testaukset ja tulokset

Kyberturvallisuuskeskuksen kybermittari- työkalun arviointi aloitettiin kybermittarin ohjeiden (Kybermittari kansallinen kyberturvallisuuden…2020, 6-7) mukaisesti valitsemalla ensiksi arvioinnin kohde. Arvioinnin kohteeksi ja osa-alueeksi valittiin koko kohdeyrityksen toiminta ja arvioinnin vetäjänä toimin minä. Kybermittarin testaus suoritettiin työpajamuotoisesti yhdessä kohdeyrityksen hallinnosta vastaavan johtaja A:n kanssa, ja tähän varattiin aikaa 2

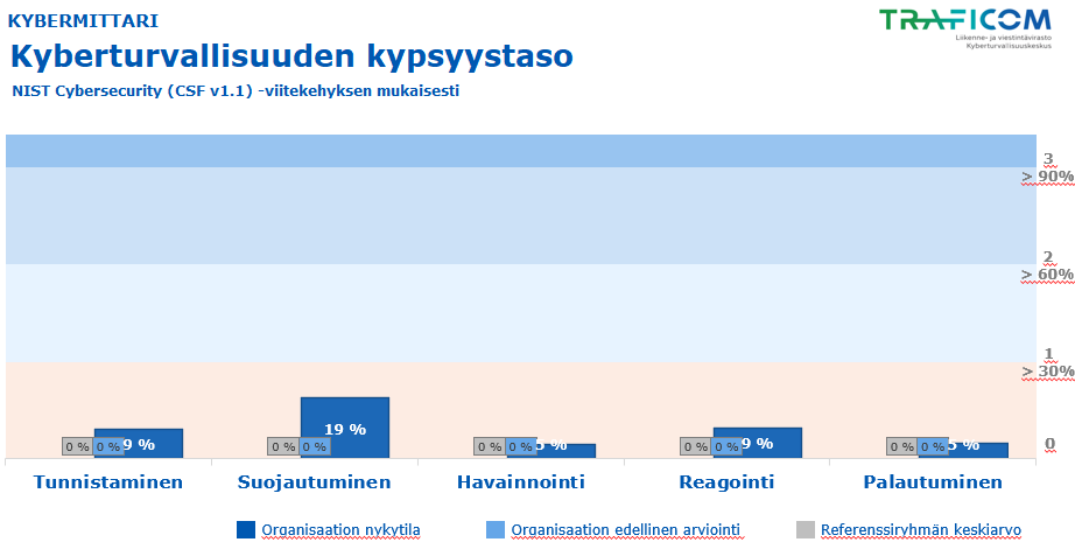
työpäivää. Tarkastelu rajoitettiin tässä testauksessa niin, ettei erikseen lähdetty kysymään ulkoistetulta IT-tuelta käytäntöjä, vaan luotettiin johtaja A:n ja minun arvioon eri käytäntöjen toteutumisesta. Kybermittarin soveltamista kohdeyritykseen tuli hieman soveltaa siitä näkökulmasta, että yritys on pieni eikä sen toiminta juurikaan vaikuta yhteiskunnan toimintaan kriittisesti. Esimerkiksi yksi mittarin testattava osa-alue liittyy yhteiskunnan kannalta kriittisten palvelujen ja toimintojen tunnistamiseen ja hallintaan, niin tämä kohta muutettiin yrityksen kannalta kriittisten palvelujen tunnistamiseen. Arvioinnissa tulee myös muistaa, ettei kohdeyrityksen missään nimessä kannatakaan tavoitella ylintä kypsyystasoa, sillä ravintola- ja tapahtuma-alan pieni yritys ei voi käyttää niin paljon resursseja kyberturvallisuuden hallintaan, ja kun sen toiminnassa ei ole yhteiskunnan toimivuuden kannalta mitään kriittistä. Kybermittari työkalun käytön tarkoituksena kohdeyritykseen on selvittää laajemmin yrityksen kyberturvallisuuden nykytilaa ja paljastaa kehityskohteita sekä tarjota mahdollinen työkalu yrityksen sovellettavaksi jatkossakin. Testauksessa tulee ottaa myös huomioon, että malli on aika ankara, sillä mikäli yksi osio koostuu vaikkapa kahdesta tavoitteesta ja toinen saa kypsyystasoksi 3 ja toinen 0, niin tulee koko osion kypsyystasoksi heikoin arvosana eli 0.



Kuvio 4: Kybertuvallisuuden kypsyystaso (Kybermittari 2022)

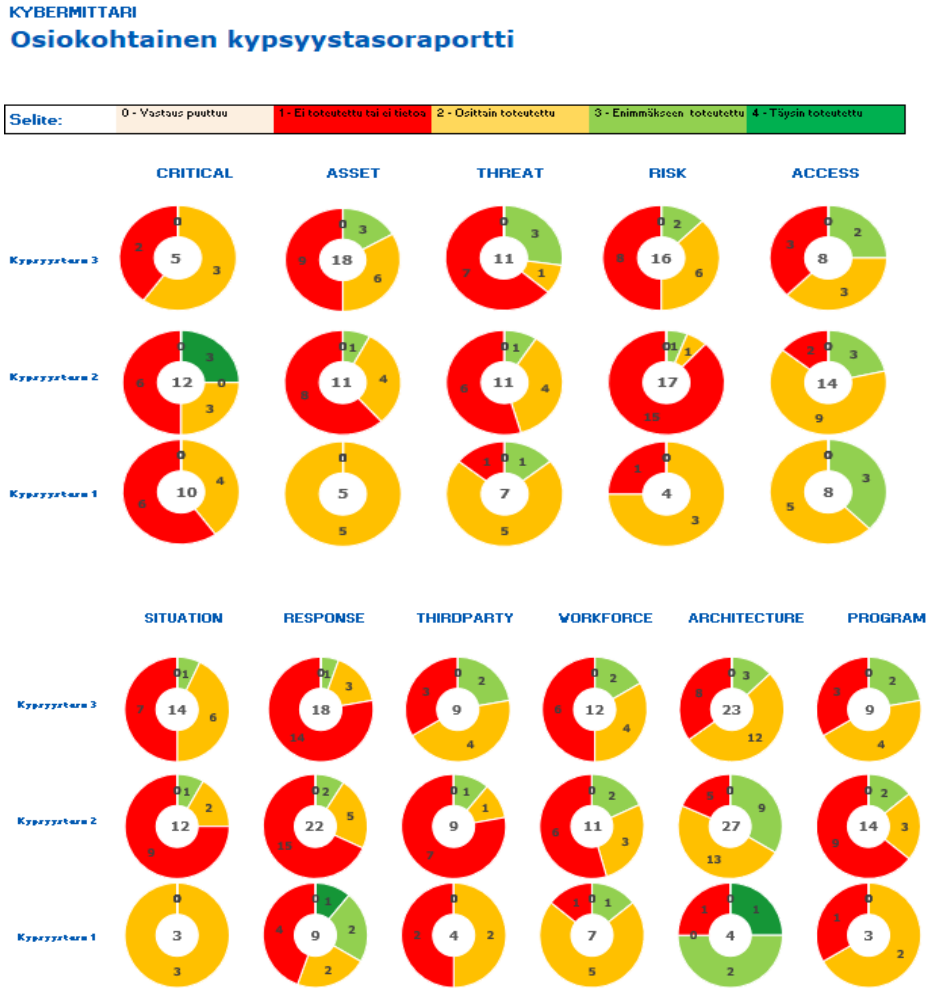
Kuten kuviosta 4 nähdään, ei yritys läpäissyt yhtäkään testausosiota, vaan jäi kaikissa osioissa kypsyystasolle 0, ja yrityksen kokonaiskypsyystasoksi testin perusteella tuli 0. Mutta tilanne ei kuitenkaan ole niin heikko, kuin tämän mukaan vaikuttaa, sillä testaus paljasti, että joitain asioita yrityksessä hoidetaan myös ihan riittävällä tasolla, mutta osion kypsyystasoksi mallissa vain niin helposti tulee 0 jos yksikin tavoite saa kypsyystasoksi 0. Esimerkiksi yrityksessä kyllä havaitaan kyberhäiriöitä ja näihin reagoidaan ja pyritään löytämään ratkaisuja, mutta kyberhäiriöiden määrittämiseen ei ole virallisia prosesseja, kriteeristöä tai rekisteriä, joten

osion kypsyystasoksi tulee 0, vaikka joitkin asiat enimmäkseen toteutuvat. Kuviosta 5 nähdään kypsyystasojen toteutuminen prosentuaalisesti NIST viitekehyksen teemojen mukaisesti. Kyberriskeiltä suojautumisesta yritys on saanut 19 %, niihin reagoinnista ja tunnistamisesta 9 % ja havainnoinnista ja palautumisesta 5 %.



Kuvio 5: Kypsyystaso NIST -viitekehyksen mukaan (Kybermittari 2022)

Kun kuviosta 6 katsoo tarkemmin osiokohtaisia kypsyystasoja, voidaan havaita keltaisesta väristä, että monet käytännöt ovat toteutuneet osittain ja myös vaalean vihreää ”enimmäkseen toteutuu” on jonkin verran nähtävissä. Osittain toteutuminen ei kuitenkaan riitä käytännön toteutumisen hyväksymiseen, minusta kuitenkin tämän yrityksen kohdalla joissain kohdissa riittää hyvin, että nämä toteutuvat osittain ja on edes jollain tapaa huomioitu. Osiokohtaisesta kypsyystasoraportista voidaan havaita, että ”ARCHITECTURE” osiossa yritys on saanut hyviä pisteitä arkaluontaisten tietojen säilyttämisestä, IT-järjestelmien eriyttämisestä OT-järjestelmistä, verkkojen suojauksesta ja verkkoliikenteen ja sähköpostin valvonnasta. ”ACCESS” osiossa enimmäkseen on toteutunut esimerkiksi pääsyvaltuuksien jako ja identiteetit, monivaiheinen/vahva tunnistautuminen kriittisiin järjestelmiin, käyttöoikeuspyynnöt ja fyysisen pääsynhallinta. Eniten punaista ”ei toteutettu” on ”RESPONSE” osiossa mikä onkin selvää, sillä yrityksellä ei ollut entuudestaan minkäänlaisia prosesseja, riskikriteeristöä, raportointia tai suunnitelmia kyberriskien varalle tai näitä tapahtumia varten ei oltu ennalta varauduttu tai harjoiteltu tai luotu minkäännäköistä jatkuvuussuunnitelmaa. Testaus paljasti kuitenkin positiivisena myös sen, että yrityksen tiedoista on saatavissa hyvät varmuuskopiot, palomuurit ja viruksentorjunta on kunnossa ja kyberhäiriöihin reagoidaan ja niitä pyritään hallitsemaan ja tätä varten on myös oikea vastuuhenkilö tiedossa.



Kuvio 6: Osiokohtainen kypsyystasoraportti (Kybermittari 2022)

Yleisesti jokaisessa osiossa yritys suoriutui hyvin ”yleisiä hallintotoimia” tavoitteesta, ja näyttäisi, että yrityksellä on hallinnollisesti hyvät valmiudet parantaa kyberturvallisuuden nykytilaa, esimerkiksi vastuut on selkeästi jaettu, ja päätöksenteko ja muutokset on nopeasti toteutettavissa matalan hierarkian yrityksessä ja yrityksestä kyllä löytyisi resursseja sekä osaamista eri käytäntöjen toteuttamiseen, mutta tätä ei vain ennen ole nähty tarpeelliseksi. Ylimmällä johdolla on hyvä näkyvyys tärkeimpiin riskipäätöksiin koko organisaatiossa ja riskienhallinnan päätöksentekijöillä on päätösvaltaa tehdä ratkaisuja itsenäisesti. Kyberhäiriöihin myös puututaan hyvin, jos poikkeamia havaitaan, mutta vasta siinä vaiheessa, jos näin tapahtuu, mutta tähän ei ole olemassa ennalta minkäänlaisia toimintaohjeita, prosesseja tai mitään ennakoivaa toimintaa. Kybermittarin testaukset nostivat myös hyvin esiin asioita, joita yrityksessä hoidetaan hyvin, vaikkakaan nämä eivät tulisi ilmi pelkästään kypsyystasojen tuloksia katsomalla.

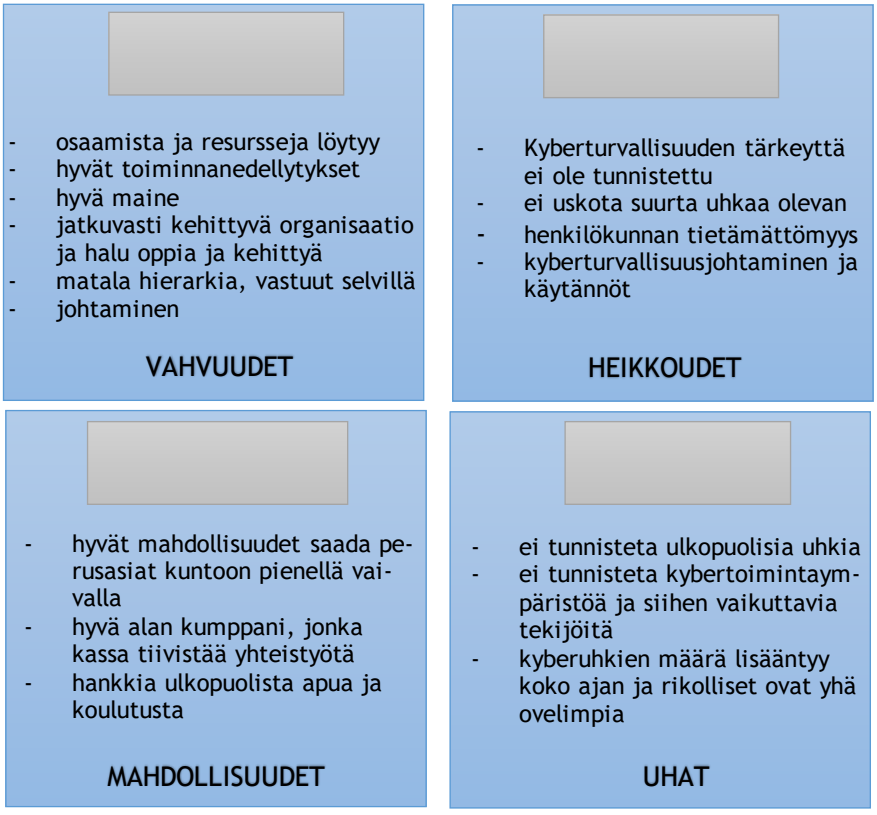
Vaikka mittarin pääasiallista kohderyhmää ovat huoltovarmuuden kannalta kriittiset yritykset, niin sen sanotaan soveltuvan käytettäväksi aivan kaikenlaisten yritysten, järjestöjen ja julkisten toimijoiden arviointiin toimialasta ja yrityksen koosta riippumatta. Kybermittaria voi myös muokata yrityksen tarpeisiin tai käyttää vain osittain. Kybermittari -työkalun testien avulla saadaan kattavasti selville yrityksen kyberturvallisuuden nykytila sekä kehittämiskohteita ja saadaan käyttöön hyvä viitekehys ja työkalu kyberturvallisuuden hallintaan jatkoakin varten. (Kybermittari kansallinen kyberturvallisuuden…2020, 3-4). Vaikka kybermittari -työkalu antoi jokaisen osion kypsyystasoksi kohdeyritykselle 0, tuloksia tarkemmin analysoitaessa paljastuu myös asioita, joita yrityksessä hoidetaan vähintäänkin kohtalaisesti enkä kuvaisi yrityksen kyberturvallisuuden nykytilaa niin heikoksi mitä testaus aluksi antaa olettaa.

6.5 Yrityksen kyberturvallisuuden nykytila

Haastattelusta ja kybermittari -työkalusta saatujen tulosten perusteella voidaan todeta, että yrityksen kyberturvallisuuden nykytila on kohtalainen. Tulokset ovat odotetun mukaisia, sillä oli entuudestaan tiedossa, ettei yrityksessä ole aiemmin juurikaan nostettu kyberasioita esiin. Analyysista paljastui kuitenkin myös hyvin hoidettuja asioita, ja että heidän apunaan on pätevä IT-alan yritys, jolle tietoturva-asiat on ulkoistettu. On hyvä, että hyödynnetään kolmannen osapuolen palveluja ja keskitytään itse siihen mihin voi eniten vaikuttaa. Yrityksen johto kuitenkin vain olettaa, että tämä kolmas osapuoli hoitaa asioita riittävällä tasolla eikä ole sen tarkemmin tietoinen minkälaisia toimenpiteitä – ja hallintaa IT kumppani toteuttaa. Yritys saisi nykytilastaan paremman kuvan tekemällä enemmän yhteistyötä kumppaninsa kanssa.

Nykytila-analyysissa tulee ottaa huomioon kohdeyrityksen toimiala, koko ja resurssit. Pienen ravintola- ja tapahtuma-alan yrityksen ei tarvitsekaan panostaa kyberturvallisuuteen niin paljon kuin vaikka sairaalan tai suuren rahoitusalan organisaation, joten on aivan ymmärrettävää, ettei kyberturvallisuus ole ollut heillä ykkösprioriteettina. Eikä tavoitteeksi tule asettaakaan, että kaikissa kybermittarin osa-alueissa päästäisiin korkeimmalle kypsyystasolle, sillä pienen ravintola-alan yrityksen ei tulisi myöskään käyttää liikaa resursseja tähän. Tämä tulee ottaa tavoitteiden asettamisessa huomioon. Nykytila-analyysissa paljastui monia heikkoja kohtia yrityksen suojauksessa sekä myös oikeasti merkittäviä uhkatekijöitä, joilla voi olla toteutuessaan ikäviä seurauksia. Analyysista paljastui kuitenkin myös positiivisia tekijöitä, ja asioita, joita yritys hoitaa jo kokonaiskuvan huomioon ottaen ihan hyvin. Huolestuttavinta Yrityksen kyberturvallisuuden tilanteessa oli tietämättömyys ja ettei asiaan oltu kiinnitetty lähes ollenkaan huomiota aiemmin. Sekin kohentaa Yrityksen kyberturvallisuuden tilaa, että lisätään tietoisuutta ja otetaan kyberturvallisuusasiat osaksi keskusteluja, ja pienellä vaivalla perusasioita kuntoon laittamalla voidaan päästä jo kohti paljon parempia tuloksia. Kybermittarin avulla nimittäin paljastui, että yrityksestä löytyisi osaamista ja resursseja kyberriskien hallintaan, mutta tätä ei vain ole valjastettu kunnolla käyttöön.

Seuraavaksi jatkan vielä nykytila-analyysia SWOT-analyysin avulla. Se on nelikenttä malli, jonka avulla voidaan analysoida yrityksen toimintakykyä ja sen toimintaympäristöä, ja sitä käytetään usein strategian laatimisen apuna sekä ongelmien tunnistamiseen, arviointiin ja uusien toimintaprosessien kehittämiseen. Yksi sen sovellus on muodostaa kokonaisvaltainen ja syvällinen tilannekuva tutkimuskohteesta. SWOT on lyhenne englanninkielisistä sanoista Strengths (vahvuudet), Weaknesses (heikkoudet), Opportunities (mahdollisuudet) ja Threats (uhat). Nelikentän vasemmalle puolelle kuvataan positiiviset asiat, oikealle puolelle negatiiviset asiat, yläpuolelle yrityksen sisäiset asiat ja alapuolelle ulkoiset asiat. Tämän pohjalta voidaan sitten tehdä päätelmiä, kuinka heikkoudet voidaan muuttaa vahvuuksiksi ja kuinka vahvuuksia voidaan käyttää hyväksi sekä miten tulevaisuuden mahdollisuuksia voidaan hyödyntää ja uhkia välttää. (Melkman & Simmonds, 2016, 132 - 133.)



Kuvio 7: Kyberturvallisuuden nykytila SWOT -nelikentässä (Melkman & Simmonds 2016,133)

Kuviossa 7 on tiivistettynä SWOT -nelikenttämalliin keskeisimmät nykytila-analyysin tulokset havainnollistamaan tuloksia helposti sisäistettävään muotoon ja hyvää pohdintaa varten. Yrityksen vahvuus kyberturvallisuuden kannalta on hyvät toimintaedellytykset ja mahdollisuudet valjastaa kyberturvallisuus paremmin mukaan organisaation toimintaan. Kybermittari paljasti, että yrityksestä löytyy esimerkiksi riskienhallintaosaamista ja monet hallinnolliset prosessit ovat kunnossa, mutta nämä puuttuvat vain kyberturvallisuuden osalta, mihin näen, että on

hyvät resurssit ja osaamista johtoportaalla ja IT-kumppanilla. Yrityksessä on myös hyvä asenne jatkuvasti kehittää toimintaa ja toimintatapoja, ja huomasin selkeän halun oppia uutta ja parantaa toimintaa, lopulta myös kyberturvallisuuden osalta. Vahvuutena näen myös yrityksen hyvän maineen vahvana toimijana alallaan, joten tämän ei pitäisi ihan pienestä tuhoutua. Heikkoudeksi koen henkilökunnan heikon osaamisen ja tietotason kyberturvallisuuden osalta. Kyberturvallisuuden tärkeyttä ei ole tunnistettu ja moniin suojaukseen, salasanoihin, käyttöoikeus- ja pääsyhallintaan liittyviin asioihin tuntui olevan hieman ”hällä väliä” -asenne vaikkakin näitä ulkoistetun IT-tuen kautta hoidettiin ihan kohtalaisesti. Yrityksessä ei myöskään uskottu, että heidän kaltaiselleen pienelle ravintola- ja tapahtuma-alan yritykselle voisi mitään vakavaa oikeasti tapahtua. Heikkoutena paljastui myös kyberturvallisuuteen liittyvien käytäntöjen, prosessien ja suunnitelmien ja ennakoivan varautumisen puuttuminen. Kyberturvallisuutta ei myöskään johdeta yrityksessä millään tasolla, mutta yrityksen vahvuudeksi muuten näen hyvän johtamistavan, mikä huokui yritysjohdon haastattelussa.

Yrityksellä siis on hyvät lähtökohdat lähteä kehittämään kyberturvallisuustoimintaa ja laittaa perusasiat kuntoon ja saada huomattavaa parannusta pienelläkin vaivalla. Yrityksellä on myös hyvä alan kumppani, jolle on ulkoistanut tietoturva-asiansa. Tämän vuoksi esimerkiksi tärkeät tiedot on asianmukaisesti suojattu ja palomuurit, virustorjunta, verkkojen suojaukset, käyttöoikeudet lähtökohtaisesti kunnossa. Kun yritys tiivistää yhteistyötä tämän kumppanin kanssa ja nostaa kyberturvallisuusasiat esiin, on tässä hyvät mahdollisuudet parantaa kyberturvallisuuden nykytilaa ja oppia alan osaajalta lisää. Yrityksessä koulutetaan paljon henkilökuntaa ja kannustetaan oppimaan uralla kokoajan lisää, joten näen kyberturvallisuuden kouluttamisen mahdollisuutena. Yrityksen kyberturvallisuuteen saadaan huomattavia parannuksia varmastikin jo sillä, että henkilökunnalle koulutetaan perusasiat ja kasvatetaan tietoisuutta ja keskustelua aiheesta. Uhkana edelleen on liian heikko kybertuvallisuusympäristön ja ulkoisten kyberuhkien tuntemus. Huijausyritysten kovaa vauhtia lisääntyessä ja rikollisten ollessa koko ajan nokkelampia, on uhkana että sellainen kyberhyökkäys toteutuu, jonka seuraukset voivat olla vakavat.

Ehdotuksia kyberturvallisuuden parantamiseksi

Nykytila-analyysi paljasti useita kehityskohtia yrityksen kyberturvallisuuteen, mutta niiden kehittäminen voi olla helpostikin toteutettavissa vahvuuksia ja mahdollisuuksia hyödyntämällä. Kirjallisuuskatsauksen, yritysjohdon haastattelun sekä kybermittari -työkalun testin perusteella olen alle listannut suosittelemani jatkotoimenpiteet yritykselle nykytila-arvion jälkeen tehtäväksi kyberturvallisuuden parantamiseksi:
6.6

- Kyberturvallisuus otetaan osaksi arkea ja johtamista

- IT-kumppanin kanssa nostetaan kyberturvallisuusasiat esiin, ja otetaan selvää paremmin mitä he tekevät kyberturvallisuuden eteen tällä hetkellä ja miten he voisivat yhdessä parantaa tätä
- Laaditaan yhdessä IT-kumppanin kanssa kybertuvallisuussuunnitelma, joka pitää sisällään ainakin yrityksen kriittiset resurssit ja niiden suojaamisen sekä toimintatavat, kuinka toimitaan, jos kyberhyökkäyksiä toteutuu ja kuinka näistä toivutaan.
- Henkilökunnalle pidetään perusasioista koulutus ja kyberturvallisuustietoisuutta lisätään sekä kyberasioista puhutaan yleisesti ja henkilökunnalle tehdään ohjeistus, kuinka toimitaan kyberuhan toteutuessa
- Vaihdetaan vanhat koneet ja järjestelmät uusiin sekä seurataan, että ohjelmistopäivitykset päivittyvät. Luodaan kaikille omat tunnukset eri järjestelmiin eikä jaeta pääkäyttäjätunnuksia muille. Pidetään salasanat piilossa omana tietona. Lopettaneiden työntekijöiden tunnukset poistetaan. (Haastattelusta selvisi, ettei näin aina ole)
- Perusasioista pidetään jatkossakin huolta ja kehitetään näitä lisää: Pidetään laitteet, järjestelmät ja ohjelmistot päivitettynä ja suojattuna, käytetään riittävän pitkiä salasanoja ja monivaiheista tunnistautumista, rajataan käyttöoikeuksia tarpeen mukaan.
- Jatkuva seuranta ja kehittäminen. Nykytila-analyysin toistetaan vuoden välein.

7 Pohdinta

Yhteenveto & loppupäätelmät

Opinnäytetyö toteutettiin toimeksiantajalle Ravintola- tapahtuma- ja matkailualan yritykselle heidän tarpeestaan kehittää kyberturvallisuuttaan, johon aiemmin ei juurikaan oltu kiinnitetty huomiota. Viime aikoina yritykseen oli kuitenkin kohdistunut jonkin verran hyökkäysyrityksiä. Yritys on kasvanut nopeaa vauhtia ja joutunut reagoimaan maailmanmyllerrykseen jatkuvasti eikä vielä ole ollut aikaa ja resursseja kyberturvallisuuteen panostamiseen eikä tätä myöskään oltu vielä nähty kovin tärkeänä. Nyt kuitenkin koettiin, että voisi olla oikea aika kehittää tätäkin osa-aluetta. Ennen kuin kyberturvallisuutta voidaan lähteä kehittämään, tuli selvittää sen nykytila, mistä lähdetään liikenteeseen. Lähtötilanne ja toimintaympäristö tulee selvittää, jotta tiedetään mitkä tietotekniset resurssit ovat tärkeimpiä yrityksen liiketoiminnan kannalta, mitä suojaustoimenpiteitä yrityksessä on jo olemassa ja mitä he tarvitsevat, mikä sitä uhkaa ja mitä kaikkea vastaan yritys taistelee. Opinnäytetyön tavoitteena oli, että tekemäni nykytila-analyysin pohjalta yritys tiedostaa lähtökohdat, jonka jälkeen se voi laittaa kyberturvallisuuden perustason toimenpiteet kuntoon ja valjastaa kyberturvallisuuden osaksi yrityksen arkea. Tavoitteena oli pystyä kehittämään kohdeyrityksen kybertietoisuutta, ja antaa heille peruslähtökohdat ja välineet suojautua kyberhyökkäyksiltä. Opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä, jonka kokonaisuus koostui aiheen kirjallisuuskatsauksesta, yritysjohdon teemahaastattelusta, Kyberturvallisuuskeskuksen kybermittari -

7.1

työkalun testistä, tulosten analysoinnista SWOT-analyysin avulla sekä kehitysehdotusten ja jatkotoimenpiteiden esittelystä.

Työn teoriaosuus toi esiin, kuinka kyberturvallisuus on tällä hetkellä trendikäs ja ajankohtainen aihe, ja kyberhyökkäyksien ja erilaisten kyberuhkien määrä kasvaa koko ajan kovaa vauhtia. Hyökkäykset ovat yhä kehittyneempiä, monimutkaisempia sekä vaikeammin havaittavissa ja torjuttavissa, joten myös niiden haitalliset vaikutukset ovat kasvaneet. Aihetta on nostanut entisestään esiin muutokset kansainvälisessä turvallisuustilanteessa, joka on korostanut myös yritysten kybervarautumisen tärkeyttä. Myös koronaviruspandemia toi yrityksille uusia haasteita ja uusia väyliä kyberrikollisille toimia etätyöratkaisujen myötä. Opinnäytetyössä yleisimpinä kyberriskeinä esiteltiin tietojenkalastelu, haittaohjelmat ja palvelunestohyökkäykset. Merkittävänä yrityksen sisältä kumpuava uhka taas paljastui työntekijöiden huolimattomuus, tietämättömyys sekä tyytymättömyys. Kyberriskin toteutuessaan voi seurauksena olla merkittäviä vaikutuksia yrityksen talouteen, maineeseen, tietopääomaan ja jopa koko toiminnan jatkuvuuteen. Erityisesti pienyrityksille pienenkin kyberturvallisuusuhan toteutuminen voi aiheutua merkittäviä vaikutuksia, ja usein juuri ne kohteet, joita ei ole suojattu ovat houkuttelevia ja helppoja kohteita hyökätä. Kohdeyritykseksi tähän työhön halusinkin pienen yrityksen, joka ei ole niin selvä kyberhyökkäyksien kohde, jotta voin tuoda esiin ja korostaa sitä, kuinka kaikkien yritysten on tärkeä kiinnittää kyberturvallisuuteen huomiota koosta ja toimialasta riippumatta.

Turvallisuutta uhkaavaa vaaraa harvoin voidaan kokonaan poistaa eikä täydellistä turvallisuutta ole olemassa, vaan kyse on riskin vähentämisestä ja siitä paljon siihen halutaan panostaa. Teoriaosuudessa nousi esiin, että pitkälle pääsee, kun tunnistaa yleisimmät kyberriskit ja osaa perusperiaatteet sekä ihan vain käyttää tervettä järkeä. Monesti hyökkääjät onnistuvat hyödyntämään organisaatioiden perustason tietoturvapuutteita, ja monet hyökkäykset olisivat estettävissä huolehtimalla kyberturvallisuuden perustason asiat kuntoon. Kyberturvallisuuden hyvä perustaso voidaan määritellä esimerkiksi työssä esiteltyjen ISO/IEC 27000 -tietoturvastandardien tai NIST:n kyberturvallisuuskehyksen avulla, ja myös kybermittari auttaa arvioimaan yrityksen kyberturvallisuuden tilaa ja tarjoaa hyvän työkalun seurantaan ja kehittämiseen. Konkreettisia tärkeitä perustason toimenpiteitä, jotka vähintään tulisi yrityksessä olla kunnossa suojautuakseen kyberhyökkäyksiltä on monivaiheinen tunnistautuminen, tietoturvapäivityksien asennus, tietoliikenteen turvallisuuden varmistaminen, haittaohjelmilta suojautuminen, palvelunestohyökkäyksiin varautuminen, pilvipalveluiden suojaus, etäyhteyksien turvallisuus, varmuuskopiot sekä langattomien yhteyksien tarkastelu.

Jotta voidaan parantaa yrityksen kyberturvallisuutta, tulee aluksi siis luoda kattava tilannekuva, joka kertoo yrityksen nykytilan, missä tällä hetkellä mennään kyberturvallisuuden suhteen. Ylimmän johdon osallistuminen ja sitouttaminen ovat myös elintärkeässä roolissa, jotta yrityksessä päästään kohti parempaa kyberturvallisuutta. Johdon tulee ensiksi ymmärtää

kyberturvallisuuden merkitys, näyttää esimerkkiä ja lisätä tämä omalle asialistalleen sekä päätöksentekoprosesseihin, jotta kyberturvallisuutta voidaan kehittää koko organisaatiossa. Jokaisella yrityksellä tulisi myös olla jonkinnäköinen kyberturvallisuussuunnitelma, jotta voidaan varmistaa, että kaikki yrityksessä tietävät miten kyberuhkia ehkäistään ja miten toimitaan, jos uhka toteutuu. Kyberturvallisuussuunnitelman tekeminen auttaa yritystä suuntaamaan ajatukset kyberturvallisuuteen. Työssä nousi esiin myös henkilökunnan kouluttamisen ja tietoisuuden lisäämisen tärkeys, sillä monesti sanotaan, että yrityksen heikoin lenkki ovat sen työntekijät, ja suurin uhkatekijä heidän aiheuttamansa inhimilliset erehdykset. Organisaation koko henkilöstöllä on tärkeä rooli sen kyberturvallisuuden varmistamisessa ja johdolla taas sen varmistamisessa, että sen henkilöstö on tarpeeksi tietoinen kyberturvallisuuden merkityksestä organisaation toiminnalle. Kohti parempaa kyberturvallisuutta voidaan siis päästä luomalla positiivista kyberturvallisuuskulttuuria, missä kyberturvallisuus olisi perustaito ja se on otettu osaksi keskustelua ja arkea, ja siihen tietoisesti panostetaan ja jatkuvasti kehitetään.

Teoria osuuden jälkeen päästin itse tutkimukselliseen kehittämistyöhön, jossa tarkemmaksi tutkimusmetodiksi valikoitui tapaustutkimus. Tutkittavana ilmiönä, josta pyrittiin saamaan mahdollisimman syvällistä tietoa oli yrityksen kyberturvallisuuden nykytila. Menetelmänä käytettiin sekä laadullisia menetelmiä: puolistrukturoitua haastattelua ja SWOT analyysia että määrällistä kybermittaria. Puolistrukturoitu haastattelu jaettiin neljään teemaan, joita olivat: Yritysjohdon yleiskuva kyberturvallisuuden nykytilanteesta, kyberuhat ja niiden hallinta, tekniset lähtökohdat ja kyberturvallisuusosaaminen. Kysymysten sisältö luotiin kirjallisuuskatsauksen pohjalta ja niiden avulla pyrittiin saamaan mahdollisimman todenmukainen kokonaiskuva yrityksen kyberturvallisuuden nykytilasta johdon näkökulmasta. Nykytila-analyysiin hyödynnettiin myös kybermittari -työkalua, joka toteutettiin Excel tiedostoon testaamalla 11 eri osion teemoihin jaettujen eri käytäntöjen toteutumista yrityksessä. Arviointiprosessi suoritettiin työpaja muotoisesti taloudesta ja hallinnosta vastaavan johtaja A:n kanssa. Testauksen avulla saatiin selville yrityksen kyberturvallisuuden kypsyystaso. Näistä saatujen tulosten jäsentelyä jatkettiin SWOT -analyysin avulla, jossa päästiin pohtimaan yrityksen kyberturvallisuuden nykytilan vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia. Nykytila-analyysissa tuli ottaa huomioon kohdeyrityksen toimiala, koko ja resurssit. Pienen ravintola- ja tapahtuma-alan yrityksen ei tarvitsekaan panostaa kyberturvallisuuteen niin paljon kuin vaikka sairaalan tai suuren rahoitusalan organisaation eikä tähän voikaan laittaa liikaa resursseja, joten on aivan ymmärrettävää, ettei kyberturvallisuus ole ollut heillä ykkösprioriteettina.

Haastattelusta ja kybermittari -työkalusta saatujen tulosten perusteella voidaan todeta, että yrityksen kyberturvallisuuden nykytila on kohtalainen. Nykytila-analyysissa paljastui monia heikkoja kohtia yrityksen suojauksessa sekä myös oikeasti merkittäviä uhkatekijöitä, joilla voi olla toteutuessaan ikäviä seurauksia. Yritysjohdon haastattelu paljasti, ettei yrityksessä ole juurikaan ennen kiinnitetty huomiota kybertuvallisuuteen eikä yritys myöskään pitänyt tätä tärkeänä tai uskonut, että heihin kohdistuisi kovin suurta uhkaa. Yritykseen oli kuitenkin

kohdistunut useita tietojenkalastelu- ja huijausyrityksiä. Paljastui myös, että esimerkiksi käyttöoikeuksia, salasanoja ja ohjelmistopäivityksiä kohtaan asennoidutaan välillä välinpitämättömästi. Yrityksessä ei myöskään tietoisesti harjoiteta kyberriskienhallintaa, kouluteta tai tiedoteta henkilökuntaa kyberasioista eikä kyberturvallisuutta johdeta millään tasolla. Johdosta löytyy kuitenkin riskienhallintaosaamista ja yleisesti yritys on hyvin muuttuva ja oppiva organisaatio, jota johdetaan ja kehitetään hyvin.

Kybermittari antoi yrityksen kyberturvallisuuden kypsyystasoksi 0. Tarkempi tulosten analysointi kuitenkin osoitti, että yrityksen koko ja toimiala huomioiden, tehdään yrityksessä useita asioita jo ihan hyvinkin, eikä tilanne ole niin huono kuin kypsyystaso antaa olettaa. Kybermittari paljasti, että yrityksen ulkoistettu IT-tuki on hoitanut esimerkiksi IT- ja OT- järjestelmien eriyttämisen, tärkeiden tietojen asianmukaisen suojauksen, palomuurit, virustorjunnan, verkkojen suojaukset sekä käyttöoikeudet lähtökohtaisesti hyvin. Suurimpia puutteita oli yleisten toimintatapojen, suunnitelmien, seurannan ja raportoinnin olemattomuus, joiden vuoksi koko osion kypsyystasoksi tuli 0, vaikka joitain käytäntöjä se olisi läpäissytkin.

Lopuksi nykytila-analyysia jatkettiin tiivistämällä tulokset SWOT-nelikenttämalliin, josta suurimpina vahvuuksina nousi esiin yrityksen hallinnollisesti hyvät valmiudet parantaa kyberturvallisuuden nykytilaa ja tarvittavien resurssien ja osaamisen olemassaolo sekä hyvä maine ja johtaminen. Mahdollisuutena nähtiinkin kyberturvallisuuden kehittäminen yhteistyössä olemassa olevan hyvän IT-alan kumppanin kanssa ja kouluttamalla. Heikkoutena kuitenkin on, ettei kyberturvallisuuden merkitystä olla tunnistettu eikä suurta uhkaa koeta olevan. Myös henkilökunnan tietoturvaosaaminen on heikkoa. Uhkana havaittiin, ettei ulkopuolisia uhkia tunnisteta eikä kybertoimintaympäristöä hahmoteta. Kyberhyökkäysten määrä lisääntyy jatkuvasti ja rikolliset ovat yhä ovelampia, joten uhkana on kyberhyökkäys, jonka seuraukset voivat olla hyvinkin haitalliset.

Nykytila-analyysi ei pelkästään paljastanut kehityskohteita, vaan toi esiin myös asioita, joita yrityksessä tehdään jo ihan heille riittävällä tasolla. Kehityskohtiin tarttumalla vahvuuksia hyödyntäen, on yrityksellä hyvät mahdollisuudet suojautua jatkossa kyberuhilta paremmin. Yrityksestä kuitenkin löytyi nyt halukkuutta kehittää kyberturvallisuuttaan ja tekemäni nykytila-analyysi on tässä ensimmäinen askel, jonka jälkeen yritys voi edetä kehitysehdotusteni mukaisesti. Jatkotoimenpiteinä ehdotin tiiviimpää yhteistyötä IT-alan kumppanin kanssa ja kyberturvallisuussuunnitelman laatimista yhdessä. Kyberturvallisuusasiat tulisi ottaa mukaan arkeen ja henkilökuntaa kouluttaa ja tiedottaa perusasioista. Myös tietoturvan perustason toimenpiteet tulee jatkossakin pitää kunnossa ja kehittää näitä lisää. Kybermittarin testausta suosittelin toistettavaksi vuoden välein.

7.2 Työn eettisyys & luotettavuus

Opinnäytetyö tulee toteuttaa noudattaen eettistä työskentelytapaa ja periaatteita. Hyvään tieteelliseen tapaan kuuluu esimerkiksi, että käytetyt tiedonhankinta- ja tutkimusmenetelmät ovat tiedeyhteisön hyväksymiä, ja tutkija sitoutuu toimimaan rehellisesti ja vilpittömästi. Hyvää tieteellistä tapaa on myös lähdeviitteiden asianmukainen merkitseminen ja pätevien lähteiden käyttö, ja huomion kiinnittäminen siihen, ettei plagiointia tapahdu. Nämä ovat käytäntöjä, joita tässä työssä on huomioitu tarkasti läpi koko työn. (Vilkka 2007, 164-165.)

Tutkimustyön luotettavuutta voidaan arvioida validiteetilla, joka tarkoittaa tutkimusmenetelmän pätevyyttä eli sen kykyä mitata alkuperäistä tutkimuskohdetta. Tässä tutkimuksellisessa kehittämistyössä oli tarkoitus mitata toimeksiantajayrityksen kyberturvallisuuden nykytilaa. Tämä onnistui melko hyvin, sillä johtajien haastattelusta ja kybermittarista tuli lähes samat tulokset, ja nämä tulokset olivat loogisia ja vastasivat myös omaa sekä yrityksen ennakkokäsitystä lähtötilanteesta, eikä suuria yllätyksiä tullut. Tulokset ovat huolellisesti analysoitu. Tutkimusmenetelminä hyödynnettiin monipuolisesti sekä laadullisia menetelmiä: teemahaastattelua ja SWOT -analyysia, että määrällistä kybermittaria. Nämä menetelmät sopivat hyvin tutkimaan kyberturvallisuuden nykytilaa selittämällä ja mittaamalla, ja numeeriset ja sanalliset tulokset olivat hyvin linjassa keskenään. Tutkimuksellisessa kehittämistyössä on myös huomioitu kohdeyrityksen koko, toimiala ja resurssit. Kohdeyritys ei ole yhteiskunnan toimivuuden kannalta kriittinen toimija eikä sellainen kohde, jonka ajattelisi heti ensimmäisenä joutuvan kriittisen kyberhyökkäyksen kohteeksi. Tämä varmasti vaikuttaa siihen, ettei yrityksen kyberturvallisuuden nykytila ole kummoinen eikä kyberturvallisuusasioihin ole kiinnitetty huomiota. Tämä tuli ottaa myös kybermittarin testauksissa huomioon ja soveltaa hieman mittaria esimerkiksi yhteiskunnan kannalta kriittisiin toimintoihin liittyvissä kysymyksissä. Mittaristo oli myös hyvin ankara kohdeyritykselle, ja myös tämä on huomioitu tuloksissa. Aikaisempaa tutkimusta aiheesta ei ole yrityksessä tehty, joten tuloksia ei voi verrata suhteessa aiempiin tuloksiin. Yksi luotettavuutta heikentävä tekijä voi olla, ettei IT-kumppania haastateltu tai otettu mukaan kybermittarin arviointiprosessiin. Heillä olisi voinut joihinkin asioihin olla vielä kattavammat ja yksityiskohtaisemmat vastaukset, mutta tulokset olisivat kuitenkin olleet hyvin samankaltaiset. Tässä työssä kuitenkin haluttiin keskittyä kohdeyrityksen näkemyksiin, ja seuraavassa vaiheessa yritys voi jatkaa kehittämistä yhdessä IT-kumppanin kanssa. (Vilkka 2007, 153.)

Koska opinnäytetyö on tehty yhteistyöyritykselle, täytyi huomioida myös heidän eettiset säätönsä ja tehdä sopimus toimeksiantajan kanssa. Haastattelut on toteutettu anonyymisti ja haastateltavien on annettu itse päättää haastatteluun osallistumisesta. Olemme etukäteen keskustelleet haastatteluun suostumisesta, ja toin ilmi osallistumisen vapaaehtoisuuden sekä tutkimuksen tarkoituksen ja tavoitteet. Haastattelu on litteroitu sanasta sanaan välttäen omien johtopäätöksien tekemistä ja näin myös tulosten luotettavuutta parantamaan.

Litteroitu aineisto ja nauhoite tuhottiin heti tulosten analysoinnin jälkeen. Vaikka tutkimuksessa haastateltiin vain kolmea kohdeyrityksen henkilöä ryhmähaastatteluna, edustivat nämä yrityksen johtajina ja osakkaina hyvin yritystä. Teemahaastattelu ehkäisee hyvin mahdollisia kysymystenasettelun väärinymmärryksiä ja antaa mahdollisuuden täydentäville kysymyksille, ja tarkoituksena olikin, että haastattelussa voidaan yhdessä pohtia asioita ja keskustelu saa lähteä rönsyilemään. Kirjallisuuskatsaukseen aiheeseen liittyvää aineistoa oli hyvin monipuolisesti saatavilla niin englannin- kuin suomenkielisenä. Taustateoriassa käytin paljon kansallisten ja kansainvälisten virastojen lähteitä, tietojen luotettavuuden ja ajankohtaisuuden vuoksi, ja näistä sai myös hyvin selville viranomaisten suosittelemat ohjenuorat. (Vilkka 2007, 164-165, 153.)

Lähteet

Painetut

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Ojasalo, K., Moilanen, T., & Ritakoski, J. 2015. Kehittämistyön menetelmät. Sanoma Pro Oy.

Vilkka, H. 2007. Tutki ja mittaa: määrällisen tutkimuksen perusteet. Helsinki: Tammi.

Sähköiset

AIG. 2022. Taking control of cyber risk. Viitattu: 07.10.2022. https://boarda-genda.com/2019/03/28/taking-control-of-cyber-risk/

Allison, A. 2014. Chapter 2: Introduction. Teoksessa: Intitute of Risk management. Cyber Risk: Resources for Practitioners. Viitattu: 20.08.2022. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Cybernews. 2022. World Economic Forum finds that 95% of cybersecurity incidents occur due to human error. Viitattu: 16.01.2023. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

Enisa Threat Landscape 2021 April 2020 to mid-July 2021. 2021. Viitattu 22.08.2022. file:///C:/Users/PinkaKantanen/Downloads/ENISA%20Threat%20Landscape%202021.pdf

Framework for Improving Critical Infrastructure Cybersecurity. 2018. Cybersecurity, Critical Infrastructure. Viitattu 15.01.2023. https://nvl-pubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

F-Secure. 2022 a. What is cyber security? Viitattu 26.09.2022. https://www.f-secure.com/fi/home/articles/what-is-cyber-security

F-Secure. 2022 b. What is a distributed denial of service attack (DDoS)? Viitattu: 07.10.2022. https://www.f-secure.com/en/home/articles/what-is-ddos

Gregory, T. 2014. Foreword. Teoksessa: Intitute of Risk management. Cyber Risk: Resources for Practitioners. Viitattu: 22.08.2022. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Isotalo, V. 2018. Mitä on kyberturvallisuus tänään? Viitattu: 02.09.2022. https://lounea.fi/lounea/artikkelit/mita-kyberturvallisuus-tanaan

ISO 27001:2005. 2005. Information technology — Security techniques — Information security management systems — Requirements. ISO/EIC

Katakri 2020 tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. Viitattu 17.08.2022. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Kybermittari – esittely. 2020. Viitattu: 31.08.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_v1.pdf

Kybermittari Kansallinen kyberturvallisuuden arviointimalli – Käyttöohje. 2020. Traficom. Viitattu: 20.08.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_K%C3%A4ytt%C3%B6ohje_V1.pdf

Kybermittari arviointityökalu_A2.0. 2022. Työkalu ladattavissa https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari?toggle=Mik%C3%A4%20on%20Kybermittari%3F

Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa ohje johdolle ja asiantuntijoille 2022. Traficomin julkaisuja 8/2022. Viitattu 07.10.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuuden_vahvistaminen_suomalaisissa_organisaatiossa_-_ohje_johdolle_ja_asiantuntijoille.pdf

Kyberturvallisuus ja yrityksen hallituksen vastuu 2020. Traficomin julkaisuja 2/2020. Viitattu: 20.08.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kärkkäinen, A. 2020. Mihin kyberturvallisuuden johtaminen kulminoituu? Viitattu 21.09.2022. https://www.cinia.fi/blogi/mihin-kyberturvallisuuden-johtaminen-kulminoituu

Laki henkilötietojen käsittelystä 1054/2018. Viitattu 20.09.2022. https://www.finlex.fi/fi/laki/alkup/2018/20181054

Laki sähköisen viestinnän palveluista 917/2014. Viitattu. 20.09.2022. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 20.09.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Luottotietolaki 527/2007. Viitattu 20.09.2022. https://www.finlex.fi/fi/laki/ajantasa/2007/20070527

Melkman, A. & Simmonds, K. 2016. Strategic Customer Planning: How to Develop and Implement a Strategic Account Plan. A specially commissioned report. Lontoo: Thorogood Publishing Ltd.

Merenkulun kyberturvallisuus – varustamojen parhaat käytännöt. Huoltovarmuusorganisaatio. 2021. Viitattu 21.09.2022. https://www.huoltovarmuuskeskus.fi/files/dd6e8c7f90cd8163a1e18df1aa109a6394ee608b/kyberturvallisuus-varustamojen-parhaat-kaytannot.pdf

Microsoft 2022. Mitä kyberturvallisuus on? Viitattu 20.08.2022. https://support.microsoft.com/fi-fi/topic/mit%C3%A4-kyberturvallisuus-on-8b6efd59-41ff-4743-87c8-0850a352a390

Nayyar, A., Rameshwar, R., & Solanki, A. 2020. Internet of Things (IoT) and the digital business environment: a standpoint inclusive cyber space, cyber crimes, and cybersecurity. In *The Evolution of Business in the Cyber Age* (pp. 111-152). Apple Academic Press.

Pienyritysten kyberturvallisuusopas 2020. Traficomin julkaisuja 228/2020. Viitattu 21.08.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Tietosuojalaki 1050/2018. Viitattu 20.09.2022. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Ulkoministeriö. 2022. Kyberturvallisuus ja kybertoimintaympäristö. Viitattu 25.08.2022. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

VAHTI 5/2013 Päätelaitteiden tietoturvaohje. 2020. Viitattu 15.01.2023. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-52013-paatelaitteiden-tietoturvaohje

VTT 2022. Kyberturvallisuus. Teknologian tutkimuskeskus. Viitattu: 20.09.2022. https://www.vttresearch.com/fi/palvelut/kyberturvallisuus

Williams, C. 2014. Chapter 1: Executive Summary – cyber risk and risk management. Teoksessa: Intitute of Risk management. Cyber Risk: Resources for Practitioners. Viitattu: 20.08.2022. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

Yleinen tietosuoja-asetus 2016/679. Viitattu 20.09.2022. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32016R0679

Kuviot

Liitteet

Liite 1: Kohdeyrityksen haastattelu

Yritysjohdon yleiskuva kyberturvallisuuden nykytilanteesta

1. Millainen on kyberturvallisuuden nykytila mielestänne yrityksessä ja tulisiko sitä kehittää jotenkin?
2. Miten kyberturvallisuutta hoidetaan tällä hetkellä yrityksessänne?
3. Kuinka tärkeäksi koette kyberturvallisuudesta huolehtimisen yrityksessänne?
4. Koetteko yrityksen ympäristön kyberturvalliseksi?
5. Olisitteko valmiita taloudellisesti panostamaan kyberturvallisuuteen tai ottaa osaksi budjettia kyberturvallisuuteen satsaamisen?

Kyberuhat ja niiden hallinta

6. Mikä ovat mielestänne keskeisiä kyberturvallisuuden uhkia yrityksellenne?
7. Onko yritykseen aiemmin kohdistunut kyberhyökkäyksiä tai havaittu tietoturvaongelmia?
8. Tiedättekö mitä kyberturvallisuuteen liittyviä vaatimuksia yrityksenne on täytettävä (esimerkiksi oikeudelliset vaatimukset tai sopimusvelvoitteet)?
9. Tehdäänkö teillä etätöitä, jos tehdään, onko tähän liittyen havaittu/tiedostettu turvallisuusuhkia?
10. Onko kyberturvallisuus osa yrityksenne riskienhallintaa?

Tekniset lähtökohdat

11. Mitkä ovat mielestänne yrityksen kriittiset tietotekniset resurssit/toiminnot, joita ilman organisaatio ei selviäisi?
12. Onko teillä jotain konkreettisia käytäntöjä kyberturvallisuuden hallitsemiseen?
13. Onko teillä jotain prosesseja tärkeiden järjestelmien, tietojen tai palvelujen tunnistamiseen sekä näiden toimivuuden ja turvallisuuden seuraamiseen?
14. Oletteko tietoisia mitä järjestelmiä yrityksen eri verkoissa on ja mitkä järjestelmät ovat yhteyksissä toisiinsa, kenellä on pääsy mihinkin tietoon ja kuka omistaa minkäkin verkon tai palvelun?
15. Kuinka olette järjestäneet pääsy- ja käyttöoikeushallinnan eri järjestelmiin ja laitteisiin?

Kyberturvallisuusosaaminen

16. Kuinka kuvaisit yrityksen kyberturvallisuusosaamista?
17. Kenellä on vastuu kyberturvallisuudesta tällä hetkellä?
18. Onko yrityksen johto ja työntekijät tietoisia mahdollisista kyberuhista?
19. Koulutetaanko tai tiedotetaanko työntekijöitä kyberturvallisuuden osalta?
20. Kuinka kyberturvallisuutta johdetaan yrityksessänne?