Antti Tuomisto | Mikko Vermanen | Nico Arvela |
Juhani Naskali | Hannu Salmela | Jonna Järveläinen

Korkeakoulujen kyberturva-laboratorion liiketoimintamalli

KyberVALIOT -osahankkeen loppuraportti

Turku Centre *for* Computer Science

TUCS National Publication
No 21, December 2020

Korkeakoulujen kyberturva-laboratorion liiketoimintamalli

KyberVALIOT -osahankkeen loppuraportti

Antti Tuomisto, Mikko Vermanen, Nico Arvela, Juhani Naskali, Hannu Salmela & Jonna Järveläinen

Turun yliopiston kauppakorkeakoulu, johtamisen ja yrittäjyyden laitos, tietojärjestelmätiede, Work Informatics

TUCS National Publication
No 21, December 2020

Sisällysluettelo

1. Johdanto 1
2. Kyberturvalaboratorion prosessit 4
2.1. Työinformatiikka ja tietoturva 4
2.2. Kyberturvalaboratorion prosessit 5
2.2.1. Markkinointi ja viestintä 5
2.2.2. Asiakkuuden käynnistys 6
2.2.3. Testauksen runko 7
2.2.4. Jälkitoimet 8
2.2.5. Tuotokset (deliverables) 9
3. Kyberturvalaboratorion Business Model Canvas 11
4. Riskikartoituksen tulokset 14
4.1. Kontaktoidut yritykset ja esitietokysely 14
4.2. IoT-kyberturvallisuuskartoitus 15
4.3. Kyberturva, tietohallinto ja case 16
4.3.1. Liiketoiminnan näkökulma kyberturvariskeihin 16
4.3.2. Liiketoiminnan jatkuvuuden turvaaminen -case 17
4.4. Kyberturvallisuus mikroyrityksissä 18
5. Kyberturvalaboratorion ekosysteemistä 20
5.1. Hybridimalli kyberturvan nostamiseksi 20
Kirjallisuutta 22
Liite 1: Yleinen kyberturvariskikartoitus 24
Liite 2: IoT-kyberturvakartoitus 27
Liite 3: IoT ja tietoturva - liiketoimintariskien kartoitus 28

Prologi

Håkan Lövdahl • 2:50 PM

Moi Antti, oli hyvä että hoksasit ottaa LLS Data mukaan tutkimukseen. Jo sen että piti vastata miten asiat on hoidettu oli tärkeää :)

Antti Tuomisto • 2:52 PM

Iso kiitos tästä palautteesta! Tämä on tärkeä viesti meille!

Håkan Lövdahl • 2:53 PM

Suomessa tarvitaan selvästi lisää tällaista.

Antti Tuomisto • 2:53 PM

Tiivistelmä

KyberVALIOT-hanke oli kolmen osatoteuttajan yhteinen hanke, joka pyrki edistämään ja kehittämään korkeakoululähtöisesti yleisesti yritysten kyberturvallisuutta ja erityisesti IoT-teknologian kyberturvaosaamista ja –tietoisuutta. Hanke toteutettiin Turun, Salon ja Kotkan seuduilla 1.9.2018-31.12.2020. Koordinaattorina toimi Turun ammattikorkeakoulu. Kymenlaaksosta osallistui XAMK:n Kotkan yksikkö ja Turun yliopistolta tietojärjestelmätiede, Johtamisen ja yrittäjyyden laitos, Kauppakorkeakoulu.

Hankkeen syntymiseen vaikutti vahvasti lisääntynyt IoT-laitteiden määrä yrityksissä, tuotteissa ja palveluissa. Välittömät laitekohtaiset ja laiteriippuvat sekä välilliset tietoturvauhat yrityksen liiketoiminnan jatkuvuudelle sekä kumppaniverkoston ja loppuasiakkaiden toiminnalle kasvoivat ja kasvavat edelleen. Hankkeen tavoite oli tuottaa pk-yrityksille, erityisesti IoT-palveluntarjoajille ja valmistavalle teollisuudelle sopivia IoT-laitteiden kyberturvaselvityksiä sekä muuten tukemaan ja edistämään yritysten IoT- ja muuta kyberturvatietoisuutta.

IoT-laitteiden testausta tehtiin sekä Turun AMK:n Salon yksikön kybertestilaboratoriossa että XAMK:n Kotkan yksikön virtuaalilaboratoriossa. Molempien laboratorioiden palveluja ja prosesseja kehitettiin teknisten ja tiedollisten toimintojen osalta toteuttamalla pilotteja alueiden yritysten tarjoamille laitteille.

Turun yliopiston toteuttama osatoteutus, jota tämä raportti kuvaa, keskittyi kyberturvallisuuden tietoisuuden edistämiseen, laboratorioiden palvelujen ja prosessien määrittelyyn, yritysrajapinnan kuvaamiseen, palvelujen tuotteistamiseen, verkostoitumiseen sekä laboratorioiden ylläpito- ja kehitystehtäviin. Yksi tavoite oli luoda kansallisesti merkittävä korkeakouluvetoinen kyberturvan edistämisen palvelu pk-yrityksille. Osahankkeen ytimessä on siten pk-yritysten tietohallinnon ja liiketoiminnan jatkuvuuden ymmärtäminen, korkeakouluyhteistyön TKI-toiminnan mahdollisuudet ja opiskelijoiden rooli yhteistyössä. Osahankkeessa tätä kyberturvalaboratorion toimintaa kuvattiin käsitteellä ulkokehä, kun Salon ja Kotkan kyberturvapalvelut ovat sisäkehää.

Osahanke tuotti kokonaisuuden ja erityisesti laboratorion liiketoimintalähtöisen kuvauksen. Lisäksi tuotettiin kyberturvatietoisuuden edistämiseksi riskikartoituspalvelu, jota testattiin XX yrityksen kanssa. Riskikartoitus ulkokehän palveluna loi luottamusta laboratorion ja yritysten välille. Lisäksi se toi useiden yritysten palautteen mukaan jo monia tärkeitä kyberturva-asioita näkyviin. Riskikartoituksesta saatujen tietojen avulla yritys voi jatkaa muihin kyberturvapalveluihin.

Tämä raportti esittelee keskeiset tulokset kyberturvalaboratorion liiketoimintamallista. Lisäksi esitellään yhteenveto hankkeessa toteutettujen riskikartoitusten ja pilottien tuloksista.

Avainsanat: kyberturvallisuus; liiketoiminnan jatkuvuus; tietohallinto; IoT.

TUCS Research Unit
UTU Information Systems Science (ISS) & Work Informatics

1. Johdanto

KyberVALIOT-hanke on kolmen osatoteuttajan yhteinen hanke, joka pyrki edistämään ja kehittämään korkeakoululähtöisesti yleisesti yritysten kyberturvallisuutta ja erityisesti IoT-teknologian kyberturvaosaamista ja –tietoisuutta. Hanke toteutettiin Turun, Salon ja Kotkan seuduilla 1.9.2018-31.12.2020. Koordinaattorina toimi Turun ammattikorkeakoulu. Kymenlaaksosta osallistui XAMK:n Kotkan yksikkö. Turun yliopistosta osallistui Kauppakorkeakoulun tietojärjestelmätiede Johtamisen ja yrittäjyyden laitokselta. Hankkeen päärahoittaja on Euroopan aluekehitysrahasto (EAKR).

Hankesuunnitelman mukaan: ”Varsinais-Suomen ja Kymenlaakson maakuntaohjelmat nostavat digitalisaation, valmistavan teollisuuden uudistumisen sekä kyberturvallisuuden tärkeimpien tavoitteiden joukkoon. KyberVALIOT (Kyberturvallisuuslaboratorio: Valmistava teollisuus ja IoT-palvelut) keskittyy digitaalisuuden valmistavalle teollisuudelle tuomiin liiketoimintamahdollisuuksiin ja tuoteturvallisuutta vaarantaviin kyberturvallisuusuhkiin. Lähtökohtana on EU-tason säädösvalmistelu, jolla pk-teollisuuden kyberturvallisuutta ja -luotettavuutta pyritään parantamaan ja varmistamaan, sekä yritysten ilmoittamat kyberturvallisuuden testaustarpeet.”

Hankkeessa hyödynnettiin alueellisia kyberturvallisuuden innovaatio- ja koulutusalustoja Salossa ja Kotkassa. Ne sisältävät IoT-kyberturvallisuuslaboratorioiden toiminnot, prosessit sekä liitynnät hankkeen ulkopuolisiin toimijoihin. Innovaatioalustojen fokuksessa hankkeessa on valmistava teollisuus sekä tietoturvalliset IoT-laitteet. Tavoitteena on luoda korkeakoulujen ja yritysten rajapintaan toiminnallinen kokonaisuus, joka kykenee tukemaan pk-yritysten IoT-liiketoiminnan kehittämistä kyberturvallisesti.

Turun yliopiston toteutuksessa tavoitteena oli luoda kyberlaboratorion toiminnalle ja palvelulle kohderyhmien tarpeita vastaava sisältö ja muoto. Hankkeen kohderyhmät ovat valmistava teollisuus ja IoT-palveluntarjoajat. Hankkeen edetessä kohderyhmiä laajennettiin koskemaan laajemmin pk-yrityksiä, koska kyberturvan ja liiketoiminnan jatkuvuuden suora ja epäsuora merkitys kasvoi entisestään. Tavoite pysyi samana: millaiset palvelut, miten toteutettuna ja miten ylläpidettyinä korkeakoulujen ja yritysten rajapinnassa ylläpitäisivät ja edistäisivät parhaiten kyberturvallisuuden tilaa verkottuneessa liiketoimintaympäristössä, työelämässä ja yhteiskunnassa hyödyntäen korkeakoulujen vahvuuksia.

Hankkeessa kyberturvapalvelujen kovassa ytimessä ns. sisäkehällä ovat Turun AMK:n ja XAMK:n laboratoriot Salossa ja Kotkassa. Salossa voidaan testata laitteita fyysisesti ja Kotka tarjoaa uniikkia virtuaalista kyberturvatestausta. Nämä asiantuntijapalvelut eroavat markkinoiden kyberturvapalveluista siinä, että ne ovat osa korkeakoulujen tutkimus- ja opetustoimintaa. Tavoite ei ole tuottaa kilpailevia sertifiointipalveluja, vaan hyvin määriteltyjä ja joustavia kyberturvaosaamisen edistämistä ja täsmätietoa tutkimukseen ja korkeakoulujen vahvuuksiin liittyen. Tämän määritelmän mukaisesti KyberVALIOT olisi oiva kumppani tietoturvapalveluja tarjoaville yrityksille, arvokas sparraaja ja keskustelukumppani IoT-laitetoimittajille ja kyberturvan edistäjä muille pk-yrityksille.

Teknologia-alallakin on tärkeää, että tutkimus- ja koulutustoiminta ovat vahvassa vuorovaikutuksessa yritysten ja työelämän kanssa. Hanke tarjoaa kolme rajapintaa kyberturvan edistämiseen erityisesti IoT-laitteiden osalta ja yleisesti liiketoiminnan jatkuvuuden turvaamisen parantamiseksi:

1. Salon fyysinen laboratorio mahdollistaa ketterät palvelut yritysten laitteiden kyberturvan kartoituksiin laitteiden elinkaaren eri vaiheissa.
2. Kotkan virtuaalialusta on sisällöltään ainutlaatuinen ratkaisu, joka voisi hyvin löytää monia uusia kumppaneita ja asiakkaita: virtuaalisesti voidaan testata monimutkaisiakin arkkitehtuureja ja ratkaisuja, muokata niitä ja testata uudelleen ilman fyysisen maailman ongelmia ja riskejä.
3. Liiketoiminnan jatkuvuuden riskikartoituksen. Turun yliopiston kauppakorkeakoulun ymmärrys tietohallinnon ja liiketoiminnan riskien kokonaisvaltaisesta arvioinnista ja kartoituksesta antaa tukea nykytilanteen selvittämiselle ja seuraavien askelien päättämiseen. Kartoitus voi jatkua Salon tai Kotkan laboratorioissa ns. sisäkehän palveluilla tai ulkokehän korkeakoulurajapinta etsii muita toimijoita edistämään yrityksen kyberturvatietoisuuden ja/tai kyberturvatilanteen parantamista.

Kokonaisuutena hanke jäsentyi kuvan 1. tavalla. Sisäkehällä ovat laboratoriot ja innovaatioalusta sisältöineen. Ulkokehällä ovat kyberturvallisuusosaaminen ja liiketoimintadiskurssi sekä asiakkuudet ja kumppanuudet.

Kuva 1. KyberVALIOT-hankkeen osat (kuva: Jarkko Paavola, 2019, Turun ammattikorkeakoulu)

Liiketoiminnallistamisen tavoitteet ja suunnittelu jakautuvat siten pilottiemme mukaisesti sisä- ja ulkokehän toimintaan. Ulkokehällä on tärkeää, että keskustelua ylläpidetään monipuolisesti elinkeinoelämän ja pk-yritysten kanssa. Jos ja kun tarpeita ilmenee, niin KyberVALIOT ei käännä selkää vaan etsii korkeakoulurajapinnasta tai

kumppaniverkostosta sopivia toimenpide-ehdokkaita ja toteuttajia kyberturvan edistämiseksi tapauskohtaisesti. Lisäksi ulkokehän tehtävä on tiedotuksen, viestinnän ja myös markkinoinnin sekä vuoropuhelun ylläpito.

Sisäkehä tarjoaa IoT-laitteisiin erikoistuneet kyberturvakartoitukset. Sisäkehän palvelut voi ottaa suoraan, mutta tarvittaessa ulkokehä auttaa kokonaiskuvan kartoituksessa ja/tai sopimusasioissa (salassapito, kustannukset, opiskelijoiden osallistuminen, muut lisäarvopalvelut).

Voimme todeta, että liiketoiminta- ja palvelunäkökulmista tässä määritelty kyberlaboratorio ja sen palvelut nähdään tarpeellisena lisänä pk-yritysten kyberturvallisuuden kehittämiseksi monitoimijaympäristössä. Sisäkehän kovat kyberturvapalvelut vaativat erikoistumista, joka aiheuttaa lisävaatimuksia teknisten kartoitusten ketterälle ja laadukkaalle toteutukselle.

Lisäksi näyttää siltä, että nykyisellään IoT-laitteita tai muita vastaavia tietoturvaspesifisiä tietoteknisiä ratkaisuja ei herkästi tarjota tämäntyyppiseen selvitykseen, vaikka ymmärrystä on niiden mahdollisista haavoittuvuuksista. Siksi ulkokehän tiedotuksellinen ja liiketoimintaa laajemmin tarkasteleva toiminta ja palvelut ovat perusteltuja: ulkokehällä on helpompi saada vuoropuhelu yrityksen kanssa käyntiin kuin pyytämällä suoraan yrityksen IoT-laite kyberturva-analyysiin.

Luvussa 2 esittelemme laboratorion prosessit, luvussa 3 liiketoimintamallin. Luvussa 4 käydään läpi toteuttamme riskikartoituspilotit ja analysoimme niiden antia ulkokehän palveluina. Luvussa 5 kokoamme kyberturvalaboratorion tuotteistamisen ideoita jatkotoimenpiteineen. Jatkokehitysideat sisältävät kyberturvalaboratorion mahdollisuuksia ja näkymiä korkeakoulurapinnassa erityisesti ulkokehän liiketoiminnan jatkuvuuden turvaamisen ja kyberturvatietoisuuden lisäämisen näkökulmista.

Hankesuunnitelmassa olimme määritelleet tavoitteeksi seuraavaa: "Lyhyen aikavälin tavoitteena on palvelukokonaisuuksien määrittely (perusskannaus, teemakohtaiset paketit, erikoiskyvykkyydet). Pitkäaikaisena tavoitteena on tuottaa innovaatioalusta, joka toimii hyvin integroituna osana alueellisia toimijoita tarjoten mielekkään palvelupolun valmistavan teollisuuden ja IoT-palveluntarjoajien kehitystarpeisiin.” Nämä tavoitteet olivat mielekkäitä, joskin käytäntö osoitti omat haasteensa tarkentaen ja muokaten tuloksiamme vastaavasti: tarvetta ja kysyntää on, mutta toimintojen ja palvelujen toteutus ja muotoilu sekä palvelujen johtaminen vaativat vielä jatkokehitystä.

2. Kyberturvalaboratorion prosessit

Hankkeen osatavoitteena oli luoda liiketoimintamalli itsenäisesti toimivalle kyberturvallisuuspalveluita tarjoavalle ja hankkeessa luotua infraa hyödyntävälle yritystoiminnalle. Tässä luvussa taustoitetaan ensin kehittämisen ja muutoksen näkökulmaa työinformatiikan käsittein. Sen jälkeen kuvataan laboratorion keskeiset prosessit: 1) Markkinointi ja viestintä, 2) Asiakkuuden käynnistys, 3) Testauksen runko sekä 4) Jälkitoimet.

2.1. Työinformatiikka ja tietoturva

Työinformatiikka (Work Informatics) on teoreettiseen ja empiiriseen tutkimukseen perustuva lähestymistapa teknologian tukeman toiminnan tarkastelemiseksi. Toisin kuin monet tietotekniikassa käytetyt lähestymistavat, työinformatiikka ei ole puhtaasti teknologiasuuntautunut vaan siinä yhdistyvät sosiologiset ja humanistiset näkemykset ihmisistä toimijoina, jotka tekevät tavoitteellista toimintaa, työtänsä, teknisten apuvälineiden välityksellä. Työinformatiikassa ei siis keskitytä ensisijaisesti teknologiaan vaan sen vaikutuksiin työssä ja toiminnassa.

Yksi lähestymistavan keskeisistä väittämistä on, että teknologian ei tule määritellä miten työtä tehdään vaan työ, sen tekijät, määrittelevät millaista teknologiaa tarvitaan. Kun puhutaan tietoturvasta ja sen tarkastelemisesta työinformatiikan lähtökohdista, tulee ymmärtää tietoturvan asettama viitekehys ja vastata kysymykseen ”kenen työstä tietoturvassa on kysymys”. Vastaus on tietysti kaikkien, mutta roolit ovat erilaisia. Siten tehtävämme saa selvästi kokonaisvaltaisemman ja kattavamman näkökulman IoT-laitteiden kyberturvaan kuin vain teknisen ulottuvuuden. Kysymys kuuluukin kyberturvalaboratorion palvelujen suunnittelussa: mistä puhutaan ja keiden kanssa, ja mitä silloin tehdään ja mistä päätetään (sillä hetkellä) ja mitä päätetään tehdä asialle seuraavaksi (yhdessä tai erikseen). Tämä toimii niin rivityöntekijän, tietoturva-asiantuntijan, toimitusjohtajan kuin kumppanin tai loppuasiakkaankin kanssa. Täytyy kuulla ja kuunnella, ja sen jälkeen toimia vastuullisesti ja asiantuntevasti. Näitä keskusteluja ja kuuntelemisia pitää olla systemaattisesti jokaisen toimijan perustoiminnassa oikealla tavalla toteutettuina. Tässä roolissa näemme kyberturvalaboratoriolle luontevan toimijan roolin.

Tietotyöläisen työ integroituu arkeen ja (työ)elämään omassa kontekstissaan siellä olevien työkalujen, sovellusten laitteiden ja infrastruktuurin parissa. Yritys, jolla on IoT-laitteita, tulisi käydä ennakoivaa ja luotettavaa kyberturvakeskustelua. Yrityksille tulisi tarjota asiantuntijapalvelua, joka mahdollistaa erilaisia mielekkäitä palvelupolkuja kyberturvan edistämiseksi. Yksi on tekninen polku eli laitteen kyberturvan testaus laboratoriossa. Muut ovat kyberturvatietoisuuden edistämisen vuoropuhelua elinkeinoelämän edustajien kanssa (Carías ym., 2020).

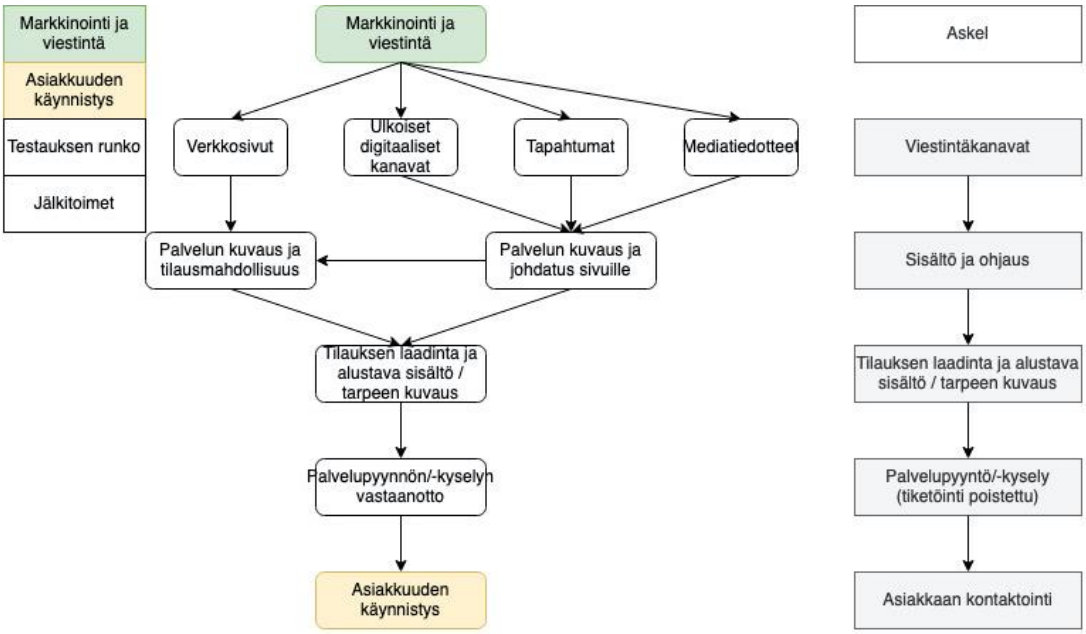
Etenkin laboratorion ulkokehällä tarkoituksen on oppia molemmin puolin ja laboratorion osalta oppimisen tulee siirtyä laboratorion toiminnan kehittämiseen tarpeita vastaavaksi. Korkeakoulujen tulee olla kyberturvassakin näkyvä, luotettava ja aktiivinen toimija pk-

yritysrajapinnassa. Jokainen yritys ja sen työntekijät toimivat tietoturvaan liittyvien haasteiden kanssa omalla tavallaan. Työinformatiikka pyrkii ottamaan tämän huomioon, kun kyberturvan edistämiseksi luodaan yhteisymmärrystä mahdollisista toteutettavista toimenpiteistä. Aina voidaan tehdä jotain ja tapaus- sekä henkilökohtaisuus ovat tärkeitä muutoksen toteuttamisessa ja onnistumisessa olevia seikkoja.

2.2. Kyberturvalaboratorion prosessit

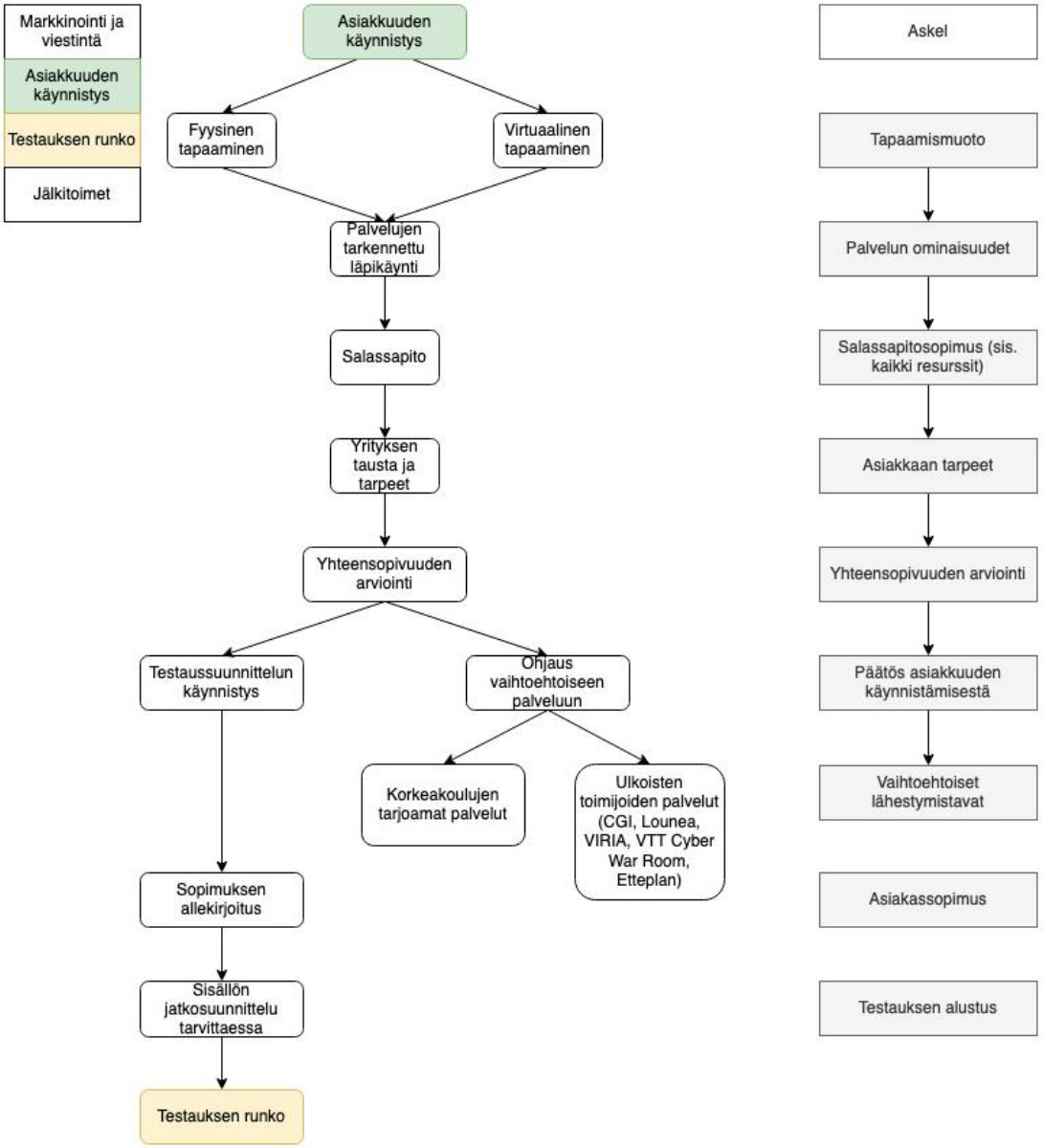
Liiketoimintamalli rakentuu nelivaiheiseen jaotteluun, jossa käsitellään ja kuvataan jatkumona 1) markkinointi ja viestintä, 2) asiakkuuden käynnistys, 3) testauksen runko sekä 4) jälkitoimet. Seuraavassa esitetään tarkennetusti kuhunkin vaiheeseen liittyvät prosessin vaiheet ja konkreettiset tuotokset.

2.2.1. Markkinointi ja viestintä



a) Viestintäkanavat: Palvelun markkinointi- ja viestintäkanavien määrittely, sis. palvelun verkkosivut, ulkoiset digitaaliset kanavat (ml. sosiaalinen media, omatoiminen viestintä), tapahtumat sekä mediatiedotteet.
b) Sisältö ja ohjaus: Viestintään ja markkinointiin liittyvä palvelun sisältökuvaus ja ohjaus yhteydenottoon ja asiakassuhteen alustusvaiheeseen.
c) Tilauksen laadinta ja alustava sisältö / tarpeen kuvaus: Tilauksen laadinta ja potentiaalisen asiakkaan kuvaama alustava tarvekuvaus.
d) Palvelupyyntö/-kysely: Palvelupyynnön vastaanotto ja prosessointi.

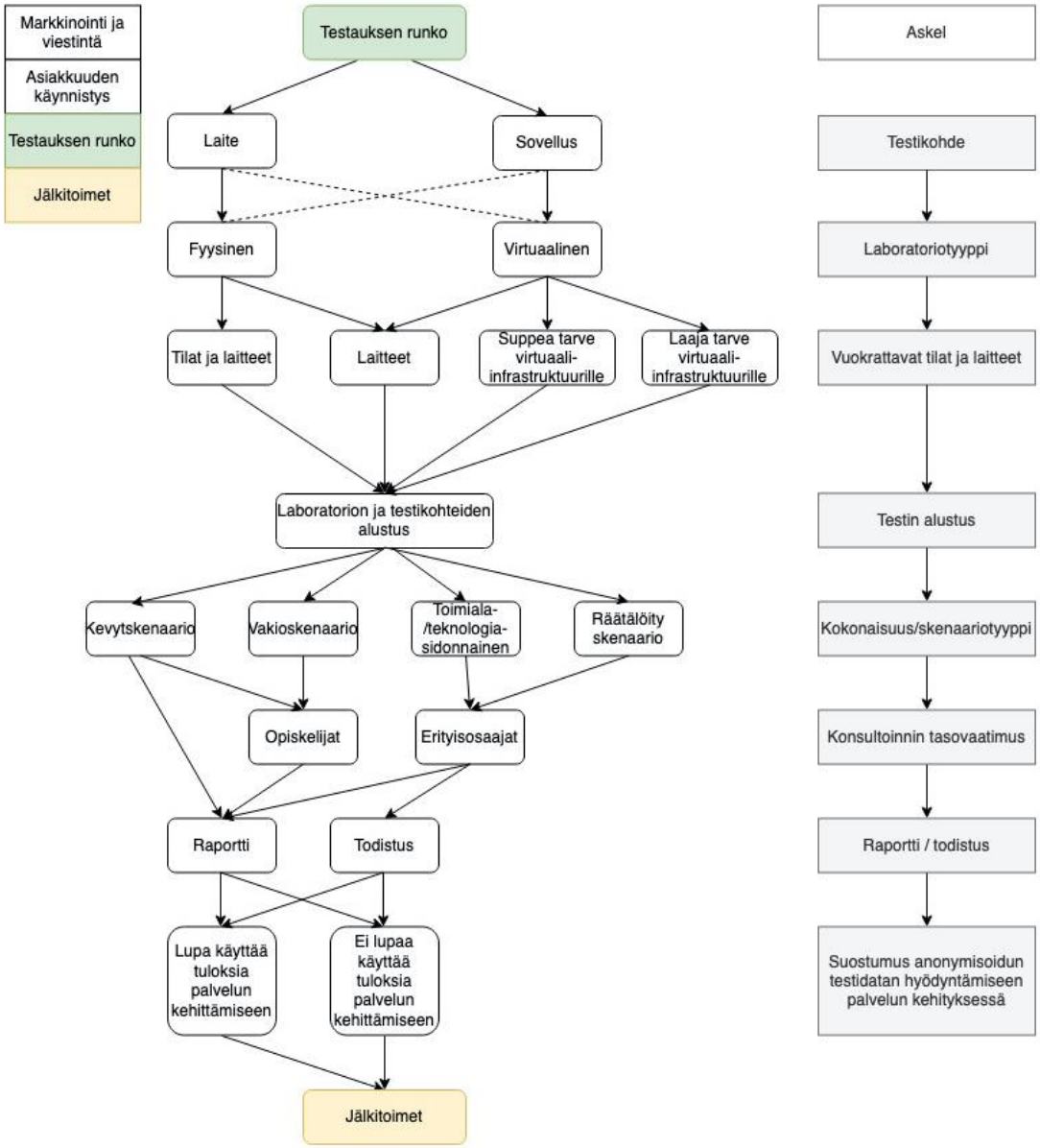
2.2.2. *Asiakkuuden käynnistys*



a) Tapaamismuoto: Potentiaalisen asiakkaan kontaktointi ja käynnistystapaamisen alustus (fyysinen / virtuaalinen).
b) Palvelun ominaisuudet: Palvelun ominaisuuksien esittely, sis. tarkennettu ja potentiaalisen asiakkaan kontekstiin soveltuvien palveluiden läpikäynti.
c) Salassapitosopimus: Salassapitosopimuksen luonti kaikkien asiakkuuteen liitännäisten toimijoiden välillä.
d) Asiakkaan tarpeet: Asiakkaan tarkennettu tarvekartoitus.
e) Yhteensopivuuden arviointi: Palvelutarjonnan ja asiakkaan tarpeiden yhteensopivuuden arviointi

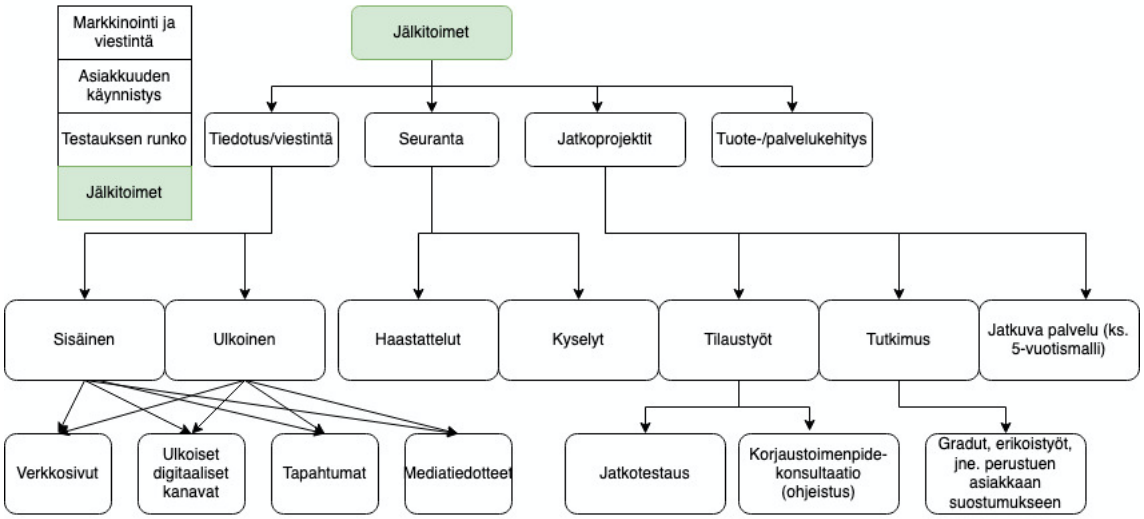
f) Päätös asiakkuuden käynnistämisestä: Mikäli palvelu ei pysty itsenäisesti tarjoamaan asiakkaan tarpeisiin riittäviä toimintoja, ohjataan nämä yhteisen kehityksen tukemiseksi muiden palveluntarjoajien piiriin osin tai kokonaisuudessaan.
g) Vaihtoehtoiset lähestymistavat: Vaihtoehtoisten lähestymistapojen määrittely (vain tarvittaessa), sis. muiden korkeakoulujen tai muiden asiantuntijaorganisaatioiden tarjoamat palvelut.
h) Asiakassopimus: Asiakassopimuksen allekirjoitus.
i) Testauksen alustus: Sis. tarpeen mukaan tarkennettu testaussuunnitelma.

2.2.3. *Testauksen runko*



a) Testikohde: Testattavan laitteen tai sovelluksen määritys ja toimitus laboratorioon, mikäli yritys ei testaa ratkaisua itsenäisesti.
b) Laboratoriotyyppi: Laboratorion valinta riippuen testattavan ratkaisun tyypistä.
c) Vuokrattavat tilat ja laitteet: Vuokrattavien resurssien määritys: a) tilat ja laitteet, b) laitteet, c) suppea tarve virtuaali-infrastruktuurille tai d) laaja tarve virtuaali-infrastruktuurille.
d) Testin alustus: Testauslaitteiston ja -tilojen alustustoimet.
e) Kokonaisuus/Skenaariotyyppi: Skenaariotyypin määritys: a) kevytskenaario, jossa toteutetaan selkeästi rajattu testauskokonaisuus, b) vakioskenaario palvelun perus testausmoduuliin perustuen, c) toimiala-/teknologiasidonnainen skenaariokokonaisuus tai d) räätälöity testiskenaario.
f) Konsultoinnin tasovaatimus: Mahdollisten konsultoitavien resurssien määritys opiskelijoiden ja erityisosaajien välillä.
g) Raportti/todistus: Testitulosten raportointi ja tarvittaessa erikseen toimitettavan todistuksen luonti ja jakelu.
h) Suostumus anonymisoidun testidatan hyödyntämiseen palvelun kehityksessä: Testidatan jatkokäytön hyväksynnän selvitys palvelun kehittämistä varten.

2.2.4. *Jälkitoimet*



- Tiedotus/viestintä: Asiakkaan suostumukseen perustuva tulosten sisäinen ja ulkoinen viestintä (referenssit) palvelun verkkosivuilla, ulkoisissa digitaalisissa kanavissa, tapahtumissa ja mediatiedotteissa.
- Seuranta: Testauksen jälkeisen asiakkaan kyberturvallisuuden kehittämisen seuranta perustuen jälkihaastatteluihin ja -kyselyihin.
- Jatkoprojektit: a) tilaustyöt (uudet testaustarpeet ja ohjaus/tuki tietoturvan konkreettisten korjaustoimenpiteiden toteuttamiseen), b) tutkimusyhteistyö (mm.

opiskelijoiden tuottamat tutkielmat ja erikoistyöt) ja c) jatkuvan palvelusopimuksen luonti erikseen määriteltävään sopimukseen perustuen.
- Tuote-/palvelukehitys: Sisäisiin havaintoihin ja kokemuksiin sekä asiakaspalautteeseen pohjautuva kyberturvallisuupalvelun kehitys.

2.2.5. *Tuotokset (deliverables)*

Kuhunkin prosessin osioon liittyvät konkreettiset tuotokset alla olevan kaavion mukaisesti:

1) Markkinointi ja viestintä
   a) Palvelun verkkosivut: Testauspalvelulle kehitetään itsenäinen verkkosivu, joka sisältää palvelun kuvauksen, testaustoiminnot ja -vaihtoehdot, hinnoittelun ja yhteydenotto-/palvelupyyntötoiminnon.
   b) Digitaalinen markkinointimateriaali:
   c) Fyysinen markkinointimateriaali:
   d) Digitaaliset jakelukanavat:
   e) Fyysiset jakelukanavat:

2) Asiakkuuden käynnistys
   a) Palvelupyyntö: Palvelupyyntö rakentuu ensisijaisesti verkkosivuilla olevan yhteydenottolomakkeen kautta. Lomakkeessa kuvataan alustava testauksen kohde (laite/sovellus) ja testaustarpeet, mikäli nämä ovat ennalta tiedossa.
   b) Alustava neuvottelu ja tarvekartoitus: Palveluntarjoaja fasilitoi fyysisen tai virtuaalisen tapaamisen, jossa käydään tarkennetusti läpi potentiaalisen asiakkaan toiminnan tausta, laitteen/sovelluksen ominaisuudet ja käyttötarkoitus ja tunnistetaan alustavat testaustarpeet
   c) Riskianalyysi: Riskikartoitus on vapaaehtoinen ja erikseen tarjottava palvelu, joka tukee mielekkään testauskokonaisuuden hahmottamista ja auttaa selvittämään potentiaalisia ongelma-alueita.

d) Laboratorion valinta: Päätös fyysisen/virtuaalisen laboratorion valinnasta tehdään aimmissa kohdissa tunnistettujen ratkaisutyypin ja testausalueiden pohjalta.
e) Testauksen laajuuden määrittely: Alkukartoituksen yhteydessä luodaan täsmällinen kuva testauskokonaisuudesta ja sen edellyttämistä toimista. Askel tukee alustavan hinnoittelun ja resursointivaatimusten määrittelyä.
f) Räätälöidyn testauksen rakenteen määrittely: Mikäli havaitaan, että testausprojekti edellyttää räätälöityä lähestymistapaa, luodaan täsmällinen suunnitelma testauksen kulusta ja taustatarpeista.
g) NDA (salassapitosopimus): Salassapitosopimus allekirjoitetaan viimeistään alkukartoituksen päätteeksi. Tilanteen vaatiessa sopimus allekirjoitetaan jo ennen kartoitusvaihetta, mikäli se edellyttää arkaluontoisten tietojen jakamista. Salassapitosopimuksen allekirjoittajat kaikki testausprojektiin liittyvät henkilöt.
h) Sopimuksen luonti: Asiakkuussopimuksessa määritellään testaukseen liittyvät toimet ja vaiheet, resursointisuunnitelma, aikataulutus sekä hinnoittelu.

3) Testauksen runko

a) Henkilöresurssien allokointi: Henkilöresurssit allokoidaan testausprojektin aikataulun ja kunkin vaiheen vaatimusten pohjalta.
b) Opiskelijaresurssien osallistaminen: Ennalta määritettyjen opiskelijaresurssien perehdytys ja vastuut määritetään ennen testausprojektin käynnistystä.
c) Laboratorion alustus: Laboratorion välineistö alustetaan testausprojektin tarpeiden mukaan.
d) Laitteen/sovelluksen toimitus: Mikäli testausprojekti toteutetaan palveluntarjoajan toimesta (vs asiakkaan omatoiminen testaus), toimitetaan laite/sovellus ennakkoon testauksen toimittajalle.
e) Skenaariopohjainen testaus: Testaus toteutetaan vaiheittain ennalta määritettyjen skenaarioiden/osakokonaisuuksien pohjalta.
f) Havaintojen kirjaus: Havainnot kirjataan ja koostetaan asiakkaalle toimitettavaan testausraporttiin.

4) Jälkitoimet

1. Testausraportin toimitus kohdeyritykselle: löydökset, vaikutukset, toimenpide-ehdotukset ja pohdiskelut.
2. Jälkineuvottelu ja tulosten läpikäynti: Testauksen löydökset käydään läpi asiakkaan kanssa raportin pohjalta, jonka jälkeen määritetään mahdolliset jatkotoimet.
3. Jatkosuunnitelman luonti: Asiakkaan tilauksesta luodaan erillinen jatkosuunnitelma esim. uusista testaustarpeista.
4. Ohjaus ulkoiseen konsultaatioon: Mikäli jatkotestaus-/korjaustoimenpiteet edellyttävät ulkoista osaamista jota testilaboratorio ei pysty tarjoamaan, pyritään asiakas ohjaamaan ulkoisten toimijoiden piiriin.
5. Testilöydösten jatkohyödyntäminen kohdeyrityksen suostumuksesta: Mikäli asiakas antaa tähän luvan, hyödynnetään testituloksia ym. havaintoja sisäisen läpikäynnin kautta palvelun kehittämisessä.
6. Tuloksista uutisointi/tiedotus kohdeyrityksen suostumuksesta:

3. Kyberturvalaboratorion Business Model Canvas

Business Model Canvasin avulla selvitimme taustaa ja sisältöä koskien kyberturvallisuuspalvelun avainkumppanuuksia, avaintoimintoja, avainresursseja, arvolupausta, asiakassuhteita, markkinointikanavia, asiakasryhmiä, kustannusrakennetta sekä tulovirtoja.

Kuva 2. Kyberturvalaboratorion liiketoimintamalli (BMC)

Avainkumppanuuksien osalta tunnistimme neljä olennaista toimijaa. Hakkerointiin keskittyneet yhteisöt, joissa ilmiötä tutkitaan organisaatioiden ja yksilöiden aseman turvaamisen näkökulmasta, nähtiin yhtenä potentiaalisena kumppaniverkoston osana. Yhteisöjen sitoutumattomuus ja kiinnostus uusiin ilmiöihin avaa palvelun näkökulmasta kehittäviä tarkastelu- ja kehitysalueita, joita palvelun jalostuksessa pyritään huomioimaan niiden kattavuuden ja ajankohtaisuuden takaamiseksi. Suuret teknologia- ja ohjelmistotoimittajat pystyvät vastaavasti tarjoamaan osaamista ja tietoa, joita palvelumme resursseilla ja toiminta-alueella ei ole mahdollista tuottaa, esimerkkinä relevantit rajapintakuvaukset. Palvelumme puolestaan pystyy tarjoamaan suurille yrityksille ulkoisen ja ketterästi toimivan infrastruktuurin ja resurssit omien asiakkuuksiensa ja kehitystoimiensa tueksi. Merkittävimpiä yhteistyötahoja ovat pk-sektorilla toimivat tietoturvayritykset, joille pystymme tarjoamaan sulautetusti laajemman testauskapasiteetin ja siten laajentamaan näiden omaa palvelutarjontaa. Palvelumme korkeakoulutaustan ansiosta myös opiskelijat muodostavat merkittävän kumppanuusalueen. Käytännössä nämä pystyvät osallistumaan todelliseen

liiketoimintaan kytkeytyviin asiakasprojekteihin opinnäyte- ja kurssitoiminnan puitteissa, laajentaen samalla itse palvelun resurssikapasiteettia.

Avaintoimintoihin lukeutuvat ensisijaisesti asiakkaiden itse tuottama ja palvelun tarjoama testauspalvelu. Tapauskohtaisesti pystymme tarjoamaan asiakkaille joko laboratoriotilat ja laitteiston omatoimista testausta varten tai vaihtoehtoisesti kokonaisuudessaan palvelun omin resurssein toteutetun testausprojektin. Lisäksi palvelutoimintaan sisällytetään yrityksille relevanttia tietoturvakoulutusta, jonka kannalta lisäarvoa tuottavat infrastruktuurin tarjoamat simulointimahdollisuudet. Kokonaisvaltaista tietoturvatietoisuuden kehittämistä koskien palvelumme pyrkii kehittämään kotimaisten yritysten osaamista tiedotuksen avulla.

Palvelun avainresursseja ovat sen henkilöstö sekä taustalla oleva infrastruktuuri, joka muodostuu Salossa sijaitsevasta laitetestauslaboratoriosta ja Kotkassa sijaitsevasta virtuaalilaboratoriosta. Henkilöresurssien osalta palveluun kiinnitetään joukko korkeakoulujen henkilökuntaa sekä tapauskohtaisesti opiskelijaresursseja tai ulkoisesti palkattua työvoimaa. Myös mahdollisten kumppanuuksien kautta voidaan solmia yhteen laboratorion oma henkilökunta sekä kumppanien resurssit.

Arvolupauksen osalta palvelu tarjoaa monipuolisen simulaatioympäristön asiakkaan omaan käyttöön sekä vaihtoehtoisesti kokonaan ulkoisesti toteutetun testauksen. Erityisesti IoT-laitteiden testaamisen osalta palvelussa kyetään toimittamaan laadukkaita ja verrattain edullisia tuloksia, osin palveluiden räätälöintimahdollisuuksien ansiosta. Testi- ja kartoitusprosessin yhteydessä asiakkaat pystyvät myös kartuttamaan kykyään itsenäisesti hallita uhkien käsittelyä ja liiketoiminnan riskien hallintaa. Vastaavasti palvelun tarjoama skenaarioiden simulointi- ja konkretisointimahdollisuus laajentaa mahdollisuuksia sisäistää riskien ja niihin varautumisen perusteet ja vaatimukset. Lopulta asiakkaille toimitetaan todistus, josta ilmenee miltä osin heidän tuotteensa ovat tietoturvatestattuja.

Asiakassuhteita voidaan solmia mm. korkeakoulukumppaneihin, joille laboratoriot tarjoavat hyödyllisen oppimisalustan. Tämän lisäksi mm. tarjottava tietoturvakoulutus voidaan integroida oppilaitosten kurssitarjontaan. Oletettavasti yleisin asiakkuus muodostuu kuitenkin yritysten kanssa joko kertaluontoisina tai pidempään jatkuvina sopimuksina, jotka voivat saada alkunsa julkisen markkinoinnin ohella kumppaniorganisaatioiden kontakteista ja henkilösuhteista.

Markkinoinnissa hyödynnetään ensisijaisesti sähköisiä kanavia, kuten korkeakoulujen viestintäkanavia ja sosiaalisia asiantuntija- ja yritysverkostoja. Olennaisen osan markkinoinnista muodostavat myös mahdollisten partnerien olemassa olevat asiakas- ja yhteistyöverkostot. Tämän lisäksi palvelua markkinoidaan relevanteissa yleisötapahtumissa, ml. alan messut. Markkinoinnin avulla pyritään ohjaamaan potentiaaliset asiakkaat riskikartoitusvaiheeseen, jossa selvitetään mahdolliset tietoturvan kipukohdat ja hahmotellaan mielekäs testauskokonaisuus.

Olennaisimpia asiakasryhmiä ovat pk-sektorin yritykset, jotka joko hyödyntävät tai tarjoavat tietoteknisiä ja erityisesti IoT-liitännäisiä ratkaisuja ja sovelluksia. Lisäksi

palveluiden piiriin pyritään ohjaamaan tietoturvakoulutusta tuottavat tahot, joille mm. virtuaalilaboratorio tarjoaa entistä laajemmat koulutuspuitteet. Palvelun yhteistyöpainotteeseen luonteeseen perustuen tarjotaan laboratorioita myös "kilpailevilla" yrityksille, jotka voivat hyödyntää olemassa olevaa infrastruktuuria omien palveluiden laajennuksena.

Palveluun liittyviä kiinteitä kustannuksia ovat laboratoriotilat, laitteet sekä vakinaisen henkilökunnan palkkamenot. Muuttuviin kustannuksiin sisältyvät asiakkaiden perehdytykseen liittyvät, tapauskohtaisesti määrittyvät kulut, varsinaisen testauksen suorittaminen sekä koulutuksen tuottaminen. Kehitysinvestoinneilla pyritään sekä päivittämään laboratorio- ja simulaatioympäristöjä että tuottamaan asiakasprojekteissa tarpeellisiksi ilmenneitä lisäominaisuuksia.

Palvelun pääasiallinen tulovirta muodostuu projektikohtaisista testaus- ja kartoituspalveluista. Näiden lisäksi tuotetaan pitkäaikaisia tai jatkuvia sopimuksia asiakkaille, jotka haluavat kartoittaa tietoturvatilannettaan pidemmällä perspektiivillä. Osan tuloista synnyttävät myös edellä mainitut koulutustuotanto ja –tarjonta sekä näihin liittyvät erilaiset yhteistyöprojektit. Osa tuloista voitaneen, tai pitänee, koota myös AMK:n omarahoituksella osana opetuksen oppimisympäristöjä.

4. Riskikartoituksen tulokset

Riskikartoitus sisältää kolme osaa: alkukartoitus, IoT kyberturvan arviointi ja liiketoimintariskin arviointi. Osat ovat hieman päällekkäisiä, mutta teemahaastattelussa oli mahdollista yrityskohtaisesti muokata keskustelun sisältöä saatujen tietojen perusteella. Siten kokonaisuus toimi hyvin, kaikki relevantit alueet tuli käsiteltyä ja ei-relevantteja voitiin perustellusti ohittaa tai jättää vähemmälle. Usein ohitetut kohdat kyllä mainittiin ja päätös sivuutuksesta tehtiin siten tavallaan yhteistymmärryksessä. Tätä kartoituksen joustavuutta ja ketteryyttä, ehkä toisin sanoin asiantuntemusta ja ymmärrystä liiketoiminnasta ja aiheesta, kiiteltiin.

4.1. Kontaktoidut yritykset ja esitietokysely

Hankkeen aikana kontaktoimme noin 175 yritystä, valtaosa näistä oli Varsinais-Suomen alueella sijaitsevia. Kartoitimme esitietokyselyn avulla yritysten kyberturvallisuuden nykytilan tasoa ja merkittävyyttä. Saimme esitietokyselyyn 15 vastausta ja näiden perusteella teimme seuraavia alustavia havaintoja:

- Yritykset kokevat kyberturvauhat yleisesti merkittäviksi. Oman henkilökunnan riski kyberturvauhkana koetaan vähäisenä ja suurin riski tulee ulkopuolisista toimijoista.
- Merkittäviä riskejä koetaan tulevan seuraavista osa-alueista: ohjelmistojen valmistusviat ja väärinkäyttö, haittaohjelmat sekä yrityksen tietojen vuotaminen. Myös tietoliikenteen turvallisuus mietityttää jonkun verran yrityksiä.
- Tietoturvallisen liiketoiminnan osoittaminen todistuksen tai sertifikaatin avulla koetaan hyvin tärkeäksi sisäisesti, asiakkaille ja yhteistyökumppaneille.
- Tietoturvallisen liiketoiminnan kartoittamiseen ja osoittamiseen yritykset ovat valmiita panostamaan vaihtelevasti jostain sadoista euroista useisiin tuhansiin euroihin.

Esitietokyselyyn vastanneista yrityksistä 13 haastateltiin ja yrityksille tehtiin kyberturvallisuuden riskikartoitus (liite 1). Etenkin pienikokoisten yritysten on tärkeää identifioida tarkkaan oikeat kohteet rajallisten resurssien käyttämiselle. Tämä on erityisen hankalaa kyberturvallisuuden alalla, sillä sen ymmärtäminen vaatii melkoisesti asiantuntijuutta. Riskikartoitus muodostettiin siten, että se tukee yrityksen osaajien arviointia eri kyberturvallisuuden osa-alueiden riskien koosta, ja siten kertoo mihin osa-alueeseen kannattaisi keskittyä.

Liitteessä 1 dokumentoitu yleinen riskikartoitus on toteutettu yleensä puhelin-haastatteluna. Haastattelijoina toimi hankkeesta 2-3 asiantuntijaa ja yrityksestä osallistui 1-3 henkilöä. Haastattelun tavoite on kyberturvatietoisuuden näkyväksi tekemine läpikävelytekniikalla ja siten melko kevyesti. Kartoitus sai hyvän vastaanoton ja johti muutamissa tapauksissa sekä hankkeen toimenpiteisiin laboratorioissa ja/tai yrityksen

omiin kyberturvallisuuden parantamistoimenpiteisiin (esim. varmuuskopioiden ottaminen yms.).

Korkean tason riskikartoitus koettiin yleisesti hyväksi työkaluksi. Hankkeen aikana toteutetut riskikartoitukset tehtiin yliopiston asiantuntijoiden tukemina haastatteluina, joissa eri osa-alueiden kyberturvallisuutta käytiin läpi yhdessä.

4.2. IoT-kyberturvallisuuskartoitus

Mikäli yrityksen liiketoiminta sisälsi IoT-laitteiden valmistusta tai käyttöä, haastattelussa käytettiin IoT-kyberturvallisuuskartoitusta (liite 2). Kartoitus oli mahdollista räätälöidä tilanteen ja vastaajien vastuu- ja osaamisalueiden mukaan. Se voitiin tehdä joko liiketoiminnan tasolla tai tarkemmin esiin tulleisiin teknisiin yksityiskohtiin paneutuen.

IoT-kyberturvallisuuskartoituksen kysymykset pohjautuvat OWASP IoT-hyökkäyspinta-aloihin (https://wiki.owasp.org/index.php/IoT_Attack_Surface_Areas), jotka uudelleenjaoteltiin kuuteen osa-alueeseen:

- Tiedon tallennus ja vakioasetukset pitävät sisällään tiedon salaukseen ja datanhallintaan liittyvät kysymykset sekä vakioasetusten sisältämät mahdolliset haavoittuvuudet, kuten esimerkiksi vakiosalasanat, joita ei luoda satunnaisesti joka laitteelle.
- Laiteohjelmisto ja päivitykset sisältävät esimerkiksi käytettyjen ohjelmistokirjastojen tietoturvan sekä päivitysten seurannan ja eheyden varmistuksen.
- Fyysisten liitäntöjen ja muistin kohdalla pohditaan erinäisten laiteporttien ja käytönaikaisen muistin turvallisuutta.
- Käyttöliittymä kokoaa kysymykset laitteen, sen hallintapaneelien ja pilviliitäntöjen turvallisuudesta – niiden salauksesta, salasanoista ja syötteiden puhdistuksesta (*input sanitation*).
- Lisäksi käydään läpi rajapintojen ja muun kommunikaation turvallisuus.

Korkealla tasolla eri kategoriat voidaan käydä nopeasti läpi kahden kysymyksen suhteen:

1) Onko tietyn osa-alueen tietoturvan varmistamiseksi luotu toimintatapoja tai prosessi?
2) Onko tietoturvan varmistamiseen ja testaukseen luotu toimintatapoja tai prosessi?

Usein eri osa-alueita mietittäessä kuitenkin pohdinta jatkui hyvinkin pieniin kyberturvan yksityiskohtiin, mikäli haastattelussa oli tämän alueen asiantuntija paikalla. Molemmissa tapauksissa kyselyn jaottelu varmisti, että keskustelu kattoi kaikki osa-alueet.

Kyberturvallisuuden eri osa-alueiden läpikäynti ja riskien näkyväksi tuominen kartoituksen pohjalta on tärkeä ensimmäinen askel kyberturvallisuuden tietoisuuden

nostamiseksi ja kyberturvallisuuden kehittämiselle. Useat yritykset jatkoivat kartoituksen pohjalta yrityksen toimintatapojen kehitystä jollain osa-alueella.

4.3. Kyberturva, tietohallinto ja case

Seuraavaksi esitellään liiketoiminnan ja sen jatkuvuuden turvaamisen näkökulmaa kyberturvaan kartoituspalvelun ja esimerkin (casen) avulla. Kartoituspalvelussa tuetaan tilannetietoisuutta, kyvykkyyksiä ja päätöksentekoa haastattelun keinoin. Haastattelun teemat ovat:

A. Mistä ja miten IoT tietoa kerätään, miten talletetaan ja käsitellään?
    a. Mihin tietoa käytetään tällä hetkellä: Kuka käyttää, missä käytetään, mihin tarkoituksiin?
    b. Ollaanko tiedon käyttöä harkittu laajennettavaksi joihinkin muihin käyttötarkoituksiin?
B. Mitkä ovat sisäiset ja ulkoiset kytkökset: Asiakkaat, kumppanit, tuotanto, toimitus ja muut prosessit
C. Mitkä ovat suurimmat liiketoiminnan riskit nykyisestä tai suunnitellusta IoT:n käytöstä?
    a. Mitä toimenpiteitä tulisi tehdä, että keskeisten riskien todennäköisyys tai niistä aiheutuva haitta saadaan mahdollisimman pieneksi?

4.3.1. Liiketoiminnan näkökulma kyberturvariskeihin

Hankkeen aikana haastatteluja varten kehitettiin kaksi haastattelulomaketta (liite 3): 1) IoT ratkaisujen tietoturvan arviointi ja 2) toteutuneesta IoT riskistä aiheutuvan liiketoiminnan vaikutuksen arviointi.

IoT tietoturvan arviointi antaa kohdeyritykselle yleiskuvan sen IoT ratkaisun tietoturvan tasosta. Se on suunniteltu erityisesti sellaisille PK yrityksille, joilla ei ole omaa IT tai tietoturvaan erikoistunutta henkilöstöä. Keskeiset osat IoT tietoturvan arvioinnissa ovat:

1. Esitietojen kerääminen: tietoturvauhkien koettu todennäköisyys, koettu merkitys toiminnan ja sidosryhmien kannalta, valmius investoida tietoturvaan.

2. Tietoturvaratkaisujen yleiskartoitus: käytössä olevan kokonaisarkkitehtuurin kuvaus, toteutuneet tietoturvariskit, käytössä olevat tietoturvaa lisäävät ratkaisut: mm. sijainti ja pääsy tiloihin, käyttöoikeuksien hallinta, varmuuskopiointi, henkilöstön koulutus, riskikartoitukset ja -suunnitelmat.

3. IoT ratkaisun tekninen toteutus ja tietoturvaratkaisut: laitteen käyttötarkoitus, kerätyn tiedon tallennusasetukset, ohjelmiston päivitys- ja testausprosessi, fyysiset liitännät, käyttöliittymä, sovellusliittymät ja tietoliikenne.

IoT liiketoimintariskien kartoitus antaa kohdeyritykselle yleiskuvan sen liiketoiminnan haavoittuvuudesta - kuinka suurta haittaa toteutuva IoT tietoturvariski voisi aiheuttaa. Tässä kartoituksessa lähtökohtana on, että tietoturvariskin (myös IoT riskin) vaikutus

liiketoimintaan tapahtuu neljän tietoriskin kautta: 1) pääsy tietoon estyy tai tieto katoaa, 2) tiedon sisältö muuttuu, 3) tiedon alkuperää ei pystytä todentamaan tai 4) tieto päätyy ulkopuolisille. Tästä lähtökohdasta voidaan laatia rajallinen määrä kysymyksiä, joilla tietoturvaan liittyvät keskeiset liiketoiminnan haavoittuvuudet voidaan tunnistaa. IoT liiketoimintariskien kartoitukseen liittyy seuraavat osat:

1. Yleiset pohjustavat kysymykset: IoT toteutuksen ja IoT:llä kerätyn tiedon määrittely, mitä tietoa IoT tuottaa ja miten sitä käsitellään.

2. IoT tiedon käsittelyn virheistä aiheutuva haitta liiketoiminnan eri osa-alueilla ja kumppanuusverkostossa: asiakkaalle toimitetun tuotteen/palvelun vikaantuminen; maksuliikenteen keskeytyminen; tuotannon keskeytyminen; varastonhallinnan ja logistiikan ongelmat; tuotekehityksen ja palvelumuotoilun ongelmat.

3. IoT tiedon käsittelyn virheistä aiheutuva yleinen haitta: lainsäädännön rikkomukset, akkreditoinnin menetys, yrityksen tai tuotteen maine markkinoilla, yritysvakoilu, ml. tarjouskilpailuja varten, muu mahdollinen ongelma.

Pääsääntöisesti IoT vaikuttaa vain joihinkin liiketoiminnan osa-alueisiin, mutta näissä vaikutus voi olla vakavampi ja monisyisempi, kuin mitä tullaan ajatelleeksi siinä vaiheessa, kun IoT:n tuottamalle tiedolle etsitään uusia ja innovatiivisia käyttötapoja. Liiketoiminnan haavoittuvuuksien selvittäminen voi konkretisoida IoT riskien ja niiltä suojautumisen merkitystä liiketoiminnan johdolle, koska riskit kuvataan heille tutulla tavalla.

Paras hyöty saadaan, mikäli samalla toteutetaan sekä IoT:n tietoturvariskin, että sen liiketoimintariskin kartoitus. Tällöin pystytään tunnistamaan sekä keskeiset IoT haavoittuvuudet ja riskit, että toteutuneiden riskien liiketoiminnalle aiheuttama haitta. Kartoitukset on tehty kevyiksi, joten ne kumpikin pystytään käymään läpi esimerkiksi yhden iltapäivän aikana, vastaamiseen riittää yksi teknisten asioiden asiantuntija (tietoturvariskit) ja yksi yrityksen liiketoiminnan hyvin tunteva asiantuntija (liiketoimintariskit). Kartoituksiin liittyvät lomakkeet on kuvattu liitteissä.

4.3.2. *Liiketoiminnan jatkuvuuden turvaaminen -case*

Hankkeessa tehtiin myös tietoturvakartoituksen lisäksi jatkuvuuden hallintaan liittyviä toimenpiteitä. Seuraavassa kuvataan esimerkkitapaus: Eräs IoT-laitteensa tietoturvakartoituksen tilannut yritys toivoi myös kartoitusta jatkuvuuden hallintaansa tietotekniseltä kannalta. Jatkuvuudenhallinta tarkoittaa toimia, joilla varaudutaan etukäteen mahdollisiin yrityksen operatiivista toimintaa uhkaaviin katkoksiin ja lisäksi katkosten jälkeen tehtäviä toimenpiteitä (Herbane, Elliott, & Swartz, 2004). Katkokset voivat johtua esim. laiterikoista, toimitusketjun ongelmista, pandemioista tai tietoturvahyökkäyksistä.

Tässä tapauksessa käytimme kehittämäämme PK-yrityksille suunnattua jatkuvuudenhallinnan kartoitustyökalua, jossa yritys valitsee itselleen tärkeimmän

liiketoimintaprosessin, ja sitä tukevat sovellukset, data, IT-infrastruktuuri sekä muut voimavarat kuten keskeiset henkilöresurssit kartoitetaan. Tämän jälkeen kartoitetaan ja arvioidaan riskit ko. voimavaroille ja suunnitellaan niille tarpeelliset riskejä minimoivat toimenpiteet, kuten vaihtoehtoiset toimintatavat, infrastruktuurin kahdentaminen, varmuuskopiointi jne. Toimenpiteet kerätään lyhyeen toimintasuunnitelmaan, jonka avulla yrityksen on helppo jatkaa riskien hallintaan ja lopuksi vielä tunnistetaan jatkuvuudenhallintaprosessin uudelleen käynnistävät tapahtumat.

Hankkeessa tehty jatkuvuudenhallintakartoitus tehtiin helmi-maaliskuussa 2020 eräälle koneiden ja laitteiden valmistukseen erikoistuneelle yritykselle, joka työllistää alle 150 henkilöä Länsi-Suomessa. Kartoituksen alkuvaiheessa mukana oli yrityksen toimitusjohtaja, järjestelmäasiantuntija sekä myyntijohtaja, mutta loppuvaiheessa haastateltavana oli enää järjestelmäasiantuntija. Kartoitus kesti noin 6 tuntia ja se tehtiin kolmena eri päivänä.

Keskeiseksi liiketoimintaprosessiksi valikoitui tarjous-tilausprosessi, jota tuki neljä kriittistä tietojärjestelmää sekä tietyt excel-taulukot ja sähköposti. Osa järjestelmistä oli vanhoja ja niiden uusimisen suunnittelu oli aloitettu. Lisäksi erään järjestelmän avainhenkilö oli eläköitymässä, joten varahenkilöitä oli jo aloitettu kouluttamaan. Infrastruktuurille havaittiin myös riskejä, joista osa oli hyväksytty, esim. oli päätetty luottaa yhteen verkkokaapeliin sekä palvelimeen, mutta mobiiliyhteydet voisivat korvata verkkoyhteyden osittain ja palvelin oli sijoitettu asiantuntevaan palvelinsaliin.

Kartoituksessa kävi ilmi, että järjestelmäasiantuntija oli varsin asiantuntevasti organisoinut ja varautunut erilaisiin riskeihin, mutta häneen kulminoitui myös avainhenkilöriski. Hän oli useissa tilanteissa ainoa, joka osasi tai pystyi tekemään palautustoimia, ja hän päivysti myös toimistoaikojen ulkopuolella sekä lomillaan. Jos jotain tapahtuisi järjestelmäasiantuntijalle, organisaatio olisi todennäköisesti jonkun aikaa vaikeuksissa. Järjestelmäasiantuntijaan kuitenkin toimitusjohtaja ja muut luottivat suuresti, ja heidän jatkuvuudenhallinnan tietoisuutensa tai riskitietoisuutensa ei ollut niin suuri, että he olisivat kokeneet tärkeäksi osallistua kartoituspalavereihin. Tutkija kuitenkin jätti toimintasuunnitelman järjestelmäasiantuntijalle toivoen, että toimintasuunnitelmasta ja avainhenkilöriskistä kohdistuen järjestelmäasiantuntijaan keskusteltaisiin myös muiden organisaation avainhenkilöiden kesken.

4.4. Kyberturvallisuus mikroyrityksissä

Kartoitusten perusteella pienyrityksillä on selkeä tarve ketterille toimenpiteille kyberturvallisuuden edistämiseksi. Ensimmäiset käytännön toimet ovat yleensä hyvin yksinkertaisia, ja niillä on suuri vaikutus tietoturvariskien pienentämiselle. Etenkin mikroyritysten kohdalla laajan tietoturvakonsultaatioprojektin tilaaminen ei ole mahdollinen satsaus, ja oma osaaminen vastaavaan pohdintaan ei riitä. Kyberturvallisuuskeskuksen kehittämä kybermittari (TRAFICOM, 2020) on yrityksen itsensä täytettäväksi tarkoitettu arviointityökalu, joka tuottaa laaja-alaisen katsauksen organisaation kyberturvallisuudesta. Työkalu on kuitenkin raskas ja vaatii organisaation

edustajilta melkoista IT-osaamista, joka ei mikroyrityksissä välttämättä ole tarvitulla tasolla. Vastaavia kevyempiä työkaluja tarvitaan lisää.

ETLA:n Kyberuhat yleistyvät - Miten Suomen yritykset pärjäävät -muistio tukee tätä näkemystä kyberturvallisuusosaamisen tarpeesta. Selvityksen mukaan mikroyritysten kyberturva jää katveeseen, vaikka niiden yhteenlaskettu vaikutus Suomen kansantaloudelle on erittäin suuri. Alle 10 henkilön tietoturvasta tarvitaan lisää tietoa. (Mattila et al., 2020)

Tämän hankkeen tulosten mukaan mikroyritykset tarvitsevat myös lisää helppoja työkaluja sekä kevyttä ulkoista tukea kyberturvallisuuden parantamiseksi. Kevyenkin keskustelun satona voi usein löytyä yksinkertaisia ensimmäisiä askelia kyberturvallisuuden parantamiseksi, ja tämä voi pahimmassa tapauksessa olla yrityksen toiminnan kannalta ratkaisevaa.

Pk-sektorin yritysten rajalliset aika- ja henkilöresurssit asettavat haasteita näiden tietoturvatilanteen kehittämiselle. Vaikka yrityksillä on selvästi kiinnostusta selvittää ja parantaa tilannettaan, tarvitsevat nämä matalan kynnyksen palveluita tarpeen täyttämiseksi. Niin ikään huomattiin, että varsinaiseen testausprojektiin ryhtyminen koettiin useissa tapauksissa liian laajamittaisena toimena, mikäli tälle ei ollut nähtävissä merkittävää hyötynäkymää. Tämä korosti kahden tietoturvapalvelun ominaisuuden kriittisyyttä:

1) Riskikartoitus: Sisäänheittopalveluna toimivat riskikartoitukset tarjosivat yrityksille kevyet lähtökohdat tietoturvatilanteensa selvittämiseen ja kehittämiseen. Jo 1-2 tunnin panostuksella nämä pystyivät avustetusti tunnistamaan potentiaalisia kipukohta toiminnastaan, mikä lisäsi testausprojektin käynnistämisen perusteltavuutta.

2) Tietoturvatodistus: Jotta yritykset pystyvät hyödyntämään tietoturvatestausten tuloksia myös ulkoisesti, tunnistettiin olennaiseksi tekijäksi mahdollisuus tuottaa näille todistus tietoturvatestauksesta. Yritykset uskoivat tietoturvasertifikaatin olevan hyödyllisin konkreettinen lopputulos, mutta jo epävirallisen todistuksen uskottiin olevan eduksi oman imagon ja luotettavuuskuvan kannalta.

Näin hankkeemme tuloksissa korostuu pk-sektorin toimijoiden kaipaama tuki paitsi ulkoisen resursoinnin, myös asiantuntemuksen suhteen. Olennaista on myös kyky hinnoitella palvelut vastaamaan kohdeyritysten todellista kustannusvalmiutta. Huolellinen alkukartoitus auttaa suunnittelemaan mielekkäästi rajatun ja mahdollisimman kevyesti hinnoitellun testauskokonaisuuden, mikä kokemustemme perusteella tulee todennäköisesti nostamaan myös toteutuneiden asiakkuuksien volyymia.

5. Kyberturvalaboratorion ekosysteemistä

Käytännön testauspalveluiden ympärille on suunniteltu ja osin luotu sisäänheittotuotteen omaisia oheis- ja alustuspalveluita. Merkittävin näistä on toistaiseksi maksutta tarjottu riskikartoitus, jossa haastattelun avulla selvitetään potentiaalisen kohdeyrityksen tietoturvan kipukohdat ja pyritään hahmottamaan mielekäs testauskokonaisuus. Tämän lisäksi olemme selvittäneet, kuinka tämän palvelun ohessa ja sen tueksi pystyisimme toteuttamaan tietoturvakoulutus- ja testauspalveluita Turun AMK:n ja XAMK:n kanssa.

Laajempi kansallinen tarkastelu puoltaa KyberVALIOT-hankkeen yhtä tavoitetta: "Innovaatioalustan perustamisen ja kehittämisen toimintamallin toteutus ja testaus (operatiivisesta toiminnasta nousevien innovaatioiden käsittelymekanismit)". Nykyisellään korkeakoulujen ja yritysten yhteistoiminnallisia kyberturvallisuuden kehittämishankkeita on käynnissä useita ja monia on jo toteutettu. Tarvetta on kyberturvallisuuden parantamistoimille laajalla rintamalla, se on selvää. Mutta selvää on myös lisääntynyt tarve näiden TKI-hankkeiden ja koulutuksen lisäämis- ja kehittämistoimenpiteiden kansallinen koordinointi. Tämä tarve korostuu, kun tarkastellaan toimenpiteiden kohdetta eli mikro- ja pk-yrityksiä. Innovatiivinen hanketoiminta yhdessä korkeakoulujen kanssa alueellisesti on hyvää, mutta sen vaikuttavuus jää usein paikalliseksi ja lukumäärältään vähäiseksi.

Kokonaisuuden johtaminen, vetovastuu tai koordinointi voisi tapahtua esimerkiksi Business Finlandin ekosysteemitoimintojen kautta Allied ICT Finlandin toimesta. Mutta pelkän ylhäältä alas annetun ja johdetun tukiorganisaation lisäksi tuntuu järkevältä toteuttaa myös alhaalta ylös best practice –tyyppisiä pilotteja aikaansaavien osaajien, alueellisten kykyjen ja paikallisten tarpeiden ristitulessa: yhtä helppoa saati oikeaa vastausta tai ratkaisua ei ole, joten on järkevää toteuttaa erilaisia kokeiluja. Juuri sellainen on KyberVALIOT-hanke ollut.

5.1. Hybridimalli kyberturvan nostamiseksi

KyberVALIOT on nostanut esiin ratkaisuja (esimerkiksi Salon ja Kotkan laboratorioiden vahvuudet ja mahdollisuudet), haasteita (mm. resurssit ja onnistunut asiakkuuksien ja kumppanuuksien hoito) ja lyhyen, keskipitkän ja pitkän aikavälin tavoitteet TKI-toiminnassa (tutkimuksen ja käytännön näkökulmat).

Hankkeen kokemusten perusteella ehdotamme hybridimallia ”innovaatioiden yhteiskehittämisen menetelmien kehittämiseksi eli miten tunnistettuja tarpeita kehitetään laboratorion liiketoimintaekosysteemissä”. Yhtymäkohtia tähän ehdotukseen löytyy mm. open innovation -kirjallisuudesta (esim. Hartmann & Trott, 2009; Schutte & Marais, 2010; Carrol & Helfert, 2015; Greco ym., 2017; Ratten, 2017).

KyberVALIOT-hybridimallissa organisointi on löyhää, mutta osallistujien rooli pyritään määrittelemään suhteessa osallistujatahon toimenpiteiden luonteeseen. Siten toiminta on alustavasti taulukon 1 mukaista:

Taulukko 1. Kyberturva innovaatioalustana -hybrimallin jäsentelyä

	Lyhyt	Keskipitkä	Pitkä
Korkeakoulut	**Kokeilut, pilotit, yritysyhteistyö, täydennyskoulutus**	**Soveltava tutkimus Tuotteistus Koulutus**	Perustutkimus
Kyberturvapalveluja tarjoavat yritykset	Kumppani, mentorointi, näkyvyys, ajantasaisuus	TKI-hankkeet, kyberturvan tarpeet ja visiot	Tuote- ja palvelukehitys
Kansalliset toimijat	Näkyvyys, tiedotus, viestintä	Tuki (koordinointia, organisointia, osa-rahoitusta)	Vienti, kv.osaaminen
Mikro- ja pk-yritykset	**Osallisuus, yhteistoiminnallisuus, vuoropuhelu**	Rekrytointi, TKI, verkostoituminen, resilienssi, kestävä kasvu	Vienti, liiketoiminnan jatkuvuuden turvaaminen

KyberVALIOssa korostamme tummennettuja kohtia, koska niissä on tällä hetkellä tarvetta lisätoimenpiteille kyberturvallisuustietoisuuden ja akuutin kyberturvatilanteen parantamiseksi. Näiden akuuttien empiirissävytteisten toimenpiteiden kautta saamme myös parempaa ymmärrystä ja lisätietoa pitkäjänteisempää tutkimusta varten.

Parantaaksemme erityisesti mikro- ja pk-yritysten liiketoiminnan jatkuvuuden turvaamistoimia ja kyberturvatietoisuuden tasoa IoT-laitteidenkin parissa, väitämme että verkostomaisen liiketoiminnan, tietotyön ja tiedollajohtamisen syvällinen ymmärrys auttavat löytämään toimivia, kestäviä ja vaikuttavia yhteistoiminnalisia toimenpiteitä korkeakoulujen ja yritysten käyttöön ja edelleen kehitettäväksi. Tarve on monitahoinen ja muuttuu koko ajan, siksi toimenpiteet ja toimintamallit pitää olla vastaavasti joustavia ja systeemisiä. Tässä meillä Turun yliopiston tietojärjestelmätieteen ja työinformatiikan asiantuntijoilla ja tutkijoilla on oma vahva ja perusteltu roolimme. Jatkamme innostuneina ja mielellämme resilienttien toimenpiteiden tutkimusta ja kehittämistä kyberturvan parissa.

Kirjallisuutta

Accenture ja Norse Corp. (2020) Security breaches report. (Accenture 2019 via Norse Corp. https://norse-corp.com/map/ Viitattu 8.12.2020)

Carías, J., Borges, M., Labaka, L., Arrizabalaga, S., Hernantes, J. (2020) Systematic Approach to Cyber Resilience Operationalization in SMEs. Vol 8, 2020, IEEE Access. DOI 10.1109/ACCESS.2020.3026063

Carroll, N. & Helfert, M. (2015). "Service capabilities within open innovation" (PDF). Journal of Enterprise Information Management. 28 (2): 275–303. doi:10.1108/JEIM-10-2013-0078.

Greco, M., Locatelli, G. & Lisi, S. (2017). "Open innovation in the power & energy sector: Bringing together government policies, companies' interests, and academic essence". Energy Policy. 104: 316–324. doi:10.1016/j.enpol.2017.01.049.

Elisa Oyj (2019) IoT-teknologian hyödyntäminen yrityksissä merkittävässä kasvussa. Kyselytutkimus. Prior Konsultointi. Uutinen 15.10.2019. https://elisa.fi/yhtiotieto/uutishuone/tiedotteet/elisan-tutkimus:-iot-teknologian-hy%C3%B6dynt%C3%A4minen-yrityksiss%C3%A4-merkitt%C3%A4v%C3%A4ss%C3%A4-kasvussa/59596558925994 Viitattu 8.12.2020.

Hartmann, D., Trott, P. (2009). "Why 'open Innovation' is Old Wine in New Bottles" (PDF). International Journal of Innovation Management. 13 (4): 715–736.

Herbane, B., Elliott, D., & Swartz, E. (2004). Business Continuity Management: time for a strategic role? Long Range Planning, 37(5), 435–457. https://doi.org/10.1016/j.lrp.2004.07.011

Lehmann, S. & Buxmann, P. (2009). Pricing Strategies of Software Vendors. Business & Information Systems Engineering, 1 (6), 452-462. DOI: 10.1007/s12599-009-0075-y

Mattila J., & Ali-Yrkkö J., & Seppälä T. (2020). Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? ETLA Muistio - ETLA Brief 93.

Ojala, A. & Tyrväinen, P. (2011a). Developing cloud business models: A case study on cloud gaming. IEEE Software, 28 (4), 42-47. DOI: 10.1109/MS.2011.51

Ojala, A. & Tyrväinen, P. (2011b). Value Networks in Cloud Computing. Journal of Business Strategy, 32 (6), 40-49. DOI: 10.1108/02756661111180122OJALA, A. &

Ratten, V. (2017). Entrepreneurship, innovation and smart cities. Abingdon, Oxon. ISBN 9781138222601.

Schutte, C. & Marais, S. (2010). "The Development of Open Innovation Models to Assist the Innovation Process". University of Stellenbosch, South Africa.

Traficom (2020) Kybermittari. https://www.kyberturvallisuuskeskus.fi/fi/kybermittari. Viitattu 2.12.2020.

Tunc, C., & Hariri, S. (2015). CLaaS: Cybersecurity Lab as a Service. J. Internet Serv. Inf. Secur., 5(4), 41-59.

Tyrväinen, P. (2012). Revenue Models in Cloud Computing. In E. Prakash (Ed.), Proceedings of 5th Computer Games, Multimedia & Allied Technology Conference (CGAT 2012), 114-119. URN: http://urn.fi/URN:NBN:fi:jyu-201209112363

Liite 1: Yleinen kyberturvariskikartoitus

1. Esitiedot

1.1. Yrityksenne toimiala
- Informaatioteknologia
- Valmistava teollisuus
- Muu, mikä?

1.2. Yrityksenne suuruusluokka
- 1-10 henkilöä
- 11-50 henkilöä
- 51-250 henkilöä
- Yli 250 henkilöä

1.3. Miten merkittäväksi riskiksi koette yritykseenne kohdistuvat tietoturvauhat yleisesti? (1 = Erittäin vähäiseksi, 5 = Erittäin merkittäväksi)

1.4. Miten merkittäväksi riskiksi koette tahallisesti aiheutetut tietoturvauhat? (1 = Erittäin vähäiseksi, 5 = Erittäin merkittäväksi)
1.4.1. Työntekijöiden aiheuttama ohjelmistojen ja/tai laitteiden tahallinen väärinkäyttö
1.4.2. Yrityksen ulkopuolisten tahojen aiheuttama ohjelmistojen ja/tai laitteiden tahallinen väärinkäyttö

1.5. Miten merkittäväksi riskiksi koette tahattomasti aiheutetut tietoturvauhat? (1 = Erittäin vähäiseksi, 5 = Erittäin merkittäväksi)
1.5.1. Työntekijöiden aiheuttama ohjelmistojen ja/tai laitteiden tahaton väärinkäyttö
1.5.2. Yrityksen ulkopuolisten tahojen aiheuttama ohjelmistojen ja/tai laitteiden tahaton väärinkäyttö

1.6. Miten merkittäväksi riskiksi koette seuraavat tietoturvauhat? (1 = Erittäin vähäiseksi, 5 = Erittäin merkittäväksi)
1.6.1. Laitteiston valmistusviat
1.6.2. Laitteiston väärinkäyttö
1.6.3. Ohjelmistojen valmistusviat
1.6.4. Ohjelmistojen väärinkäyttö
1.6.5. Ohjelmistojen ja päivitysten tietoturva (myös firmware)
1.6.6. Yrityksen tietojen leviäminen/vuotaminen
1.6.7. Haittaohjelmat
1.6.8. Tietoliikenteen tietoturvan puutteellisuus

1.7. Miten tärkeäksi koette tietoturvallisuuden osoittamisen yrityksenne toiminnassa? (1 = Ei lainkaan tärkeää, 5 = Erittäin tärkeää)
1.7.1. Sisäisesti
1.7.2. Asiakkaille
1.7.3. Yhteistyökumppaneille

1.8. Minkä suuruisella taloudellisella panoksella olette valmiita kartoittamaan ja todentamaan yrityksenne tietoturvatilannetta?
- Emme ole valmiita tekemään taloudellisia panostuksia
- Enintään 100 euroa
- Enintään 500 euroa
- Enintään 1 000 euroa
- Enintään 5 000 euroa
- Enintään 10 000 euroa

2. Yleiskatsaus (läpikävely)

2.1. Alustus
- Toiminnan tausta
- Miksi tietyt laitteet/sovellukset on käytössä?
- Mikä on merkittävin järjestelmä/laite?
- Mikä järjestelmä sisältää sensitiivisintä tietoa?
- Onko järjestelmä verkossa?
- Mistä data syötetään ja mihin se johdetaan?
- Mikä on tietojärjestelmien merkitys liiketoiminnalle, millaisia ongelmia tietoturvariskit voivat aiheuttaa?
- Mikä on yrityksen tärkeintä tietoa?

2.2. Tausta
- Onko yritykseenne kohdistunut havaittuja tietoturvariskejä/-hyökkäyksiä?
- Miten ja missä vaiheessa riskit havaittiin?
- Millaisia seurauksia riskeillä/hyökkäyksillä on havaittu?

2.3. Tietoturvaosaaminen
- Minkä tasoiseksi arvioitte nykyisen tietoturvaosaamistanne?
- Koetteko ulkoisen tietoturvakonsultoinnin hyödylliseksi/tarpeelliseksi?

2.4. Sijainti ja pääsy
- Pääsevätkö asiakkaat tai toimittajat yrityksen tietojärjestelmään?
- Onko IT-infra yrityksen omissa tiloissa?
- BYOD?
- Kenellä on pääsy infraan jos pääsy omista tiloista?
- Kenellä on pääsy järjestelmään?

2.5. Riskienhallinta

- Onko yrityksellä riskinhallintastrategia tietoturvariskeille?
- Minkälaisia riskejä on tunnistettu?

2.6. Varmuuskopiointi
- Onko jonkin datan oltava jatkuvasti ajan tasalla?
- Kuinka usein varmuuskopioita tehdään?
- Miten ne tehdään?
- Missä säilytetään?
- Testataanko varmuuskopioiden toimintaa?
- Kuinka pitkään niitä säilytetään?
- Kenen vastuulla?

2.7. Konkreettiset toimet
- Onko tietojärjestelmät suojattu viruksilta?
- Pääsynhallinta? (Käytetään esimerkkinä edellä käsiteltyä järjestelmää)
- Miten valvonta on toteutettu?
- Päivitysten asentaminen?
- Kuinka nopeasti kriittiset korjaukset otetaan käyttöön?
- Miten verkkoon pääsee?
- Onko etätyö mahdollista?
- Onko olemassa tietoturvapolitiikka ja hyväksytetäänkö se henkilöstöllä?
- Tietoturvapolitiikan sanktiot?
- Onko NDA käytössä?

2.8. Henkilöstö
- Pidetäänkö henkilöstölle tietoturvakoulutuksia? Sis. uudet ja olemassa olevat
- Monelleko resurssille turvatoimet on jaettu? Vai onko osaaminen keskittynyt vain yhteen työntekijään?
- Miten tilapäinen sijaisuus/seuraajan osaaminen on hoidettu?

2.9. Suunnitelmat
- Aiotteko jatkossa tehostaa tietoturvan hallintaa?
- Näettekö konkreettisia tarpeita jatkotoimille (mitä?)

Liite 2: IoT-kyberturvakartoitus

Data storage & Default settings
Process (policy + implementation) for ensuring secure data storage and default settings?

- Testing / Confirmation?

Firmware & Updates
Process for ensuring security of update process?

- Testing / Confirmation?

Physical connections
Process for ensuring security of physical connections?

- Testing / Confirmation?

User interface
Process for ensuring secure UI and user inputs?

- Testing / Confirmation?

APIs
Process for encryption and minimizing information leaks and attack surfaces?

- Testing / Confirmation?

Communication
Process for ensuring security of network communications?

- Testing / Confirmation?

Categorized OWASP IoT Attack Surface Areas (italic) and example questions (https://www.owasp.org/index.php/IoT_Attack_Surface_Areas)

Data storage & Default settings
Local Data Storage
Ecosystem Access Control

Questions:- Do you make sure passwords are not hardcoded or weak?
- Do you have processes for user privacy protection?
- Is your data stored encrypted?
- Do you use device management?

Firmware & Updates
Device Firmware
Update Mechanism
(… continues in the next column)

Questions:
- Do you secure old software components?
- Are your updates encrypted / validated?
- How do you ensure security updates are installed?
- Do you check fw for sensitive information?

Physical connections
Device Physical Interfaces
Device Memory

Questions:
- Are physical hardening measures used?
- Open ports?
- Tested for privilege escalation?
- Cleartext memory (i.e. encryption keys)?

User interface
Device Web, Administrative, Cloud Web & Mobile Interface

Questions:
- Is encryption used?
- 2-factor-auth option?
- Is user input sanitated and validated?
- Is account lockout used?
- Are operator modifications restricted (for example with user classes)?
- (Applicable questions from Updates-cat.)

APIs
Third-party Backend APIs
Vendor Backend APIs
Ecosystem Communication

Questions:
- Does your API have authentication?
- … encryption?
- … input and output filtering?
- … non-implicit trust between components?

Communication
Device Network Services
Network Traffic

Questions:
- Is your data transferred encrypted?
- Do you make sure no insecure network services are running on your devices?
- Do you / how do you manage DoS?

Optional: Safety integrity level assessment (probability and risk)

Liite 3: IoT ja tietoturva – liiketoimintariskien kartoitus

A. YLEISET POHJUSTAVAT KYSYMYKSET

- Mistä ja miten IoT tietoa kerätään, miten talletetaan ja käsitellään? (jos tehty tietoturvakartoitus, tätä ei tarvita?)
- Mihin tietoa käytetään tällä hetkellä: Kuka käyttää, missä käytetään, mihin tarkoituksiin?
- Ollaanko tiedon käyttöä harkittu laajennettavaksi joihinkin muihin käyttötarkoituksiin?

B. OSIOKOHTAISET KYSYMYKSET

1. **Asiakkaalle toimitettavaan tuotteeseen tai palveluun liittyvät ongelmat**

   Onko IoT tieto käytössä - tai suunnitellaanko sen käyttöä - asiakkaalle tarjotun tuotteen tai palvelun osana?

   Ei: siirry osioon 2.

   Kyllä: **Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:**

   1.1 - asiakas ei voi käyttää tuotetta tai tuote toimii virheellisesti? (Kyllä/Ei)
   1.2 - asiakas ei saa virheilmoitusta tai ennakoivaa huoltopalvelua? (Kyllä/Ei)
   1.3 - asiakas ei saa toimintansa kannalta oleellisia tietoja ja analyyseja tai tiedot ovat virheellisiä? (Kyllä/Ei)
   1.4 - asiakkaan liiketoiminnalle aiheutuu muuta haittaa, mitä: _____

   Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa
   1.5 - asiakkaille/asiakkaiden liiketoiminnalle? (Vähäinen/Merkittävä)
   1.6 - tuotteen/palvelun tuottamiseen osallistuvien kumppaniyritysen liiketoiminnalle? (Vähäinen/Merkittävä)
   1.7 - yrityksen omalle liiketoiminnalle? (Vähäinen/Merkittävä)

2. Maksuliikenteen ongelmat
Onko IoT tieto käytössä - tai suunnittellaanko sen käyttöä - osana laskutus- tai laskunmaksuprosessia?

Ei: siirry osioon 3.

Kyllä: **Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:**

2.1 - yritys ei kykene lähettämään laskuja asiakkaille koska laskutustiedoissa on epäselvyyttä (Kyllä/Ei)
2.2 - yritys lähettää virheellisiä laskuja (Kyllä/Ei)
2.3 - toimittajille ei kyetä maksamaan laskuja, koska laskutustietoja ei kyetä todentamaan (Kyllä/Ei)
2.4 - toimittajille maksetaan liikaa/liian vähän (Kyllä/Ei)
2.5 - smart contract -tyyppisistä laskutusjärjesteluistä joudutaan luopumaan (Kyllä/Ei)
2.6 - laskutuksessa/laskun maksussa syntyy muu virhetilanne, mikä: ____

Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa:
2.6 - asiakkaille/asiakkaiden liiketoiminnalle? (Vähäinen/Merkittävä)
2.7 - toimittajien (laskuttajie) liiketoiminnalle? (Vähäinen/Merkittävä)
2.8 - yrityksen omalle liiketoiminnalle? (Vähäinen/Merkittävä)

3. Tuotantoprosessin ongelmat

Onko IoT tieto käytössä - tai suunnittellaanko sen käyttöä - osana yrityksen tuotantoprosessia?

Ei: siirry osioon 4.

Kyllä: **Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:**

3.1 - tuotannon kannalta olennaista tietoa ei saada kerättyä ja tuotantoprosessi keskytyy (Kyllä/Ei)
3.2 - yrityksen tuotantolaitteiden vikaantumisesta ei saada ennakoivaa tietoa ja tuotantoprosessi keskeytyy (Kyllä/Ei)
3.3 - tuotannossa syntyy laatuongelmia, hävikkiä ja/tai ylimääräisiä kustannuksia (Kyllä/Ei)
3.4 - toimitukset asiakkaille keskytyvät/viivästyvät (Kyllä/Ei)
3.5 - tuotannossa syntyy muu virhetilanne, mikä: _____

Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa:

3.6 - asiakasyrityksen liiketoiminnalle? (Vähäinen/Merkittävä)
3.7 - alihankkijoiden ja muiden tuotannon yhteistyökumppaneiden liiketoiminnalle? (Vähäinen/Merkittävä)
3.8 - yrityksen omalle liiketoiminnalle? (Vähäinen/Merkittävä)

4. Toimitusketjun ongelmat

Onko IoT tieto käytössä - tai suunnittellaanko sen käyttöä - osana varaston hallintaa ja logistiikkaa?

Ei: siirry osioon 5.

Kyllä: **Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:**

4.1 - varastosaldoja ei tiedetä ja joudutaan ostamaan/valmistamaan ylisuuria varastoja (Kyllä/Ei)
4.2 - varastosaldoja ei tiedetä ja tuotanto/toimitukset keskeytyvät (Kyllä/Ei)
4.3 - saapuvia toimituksia ei kyetä synkronoimaan tuotannon aikatauluihin (Kyllä/Ei)
4.4 - lähteviä toimituksia ei kyetä synkronomiaan asiakkaan tuotannon aikatauluihin (Kyllä/Ei)
4.5 - tietoja raaka-aineiden ja komponenttien alkuperästä tai laadusta ei saada tai tiedot ovat virheellisiä (Kyllä/Ei)
4.6 - asiakas ei saa tietoja laadusta, kuljetusolosuhteista toimitusten aikana tai komponenttien/raaka-aineiden alkuperästä (Kyllä/Ei)
4.7 - toimitusketjussa syntyy muu virhetilanne, mikä:_____

Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa:

4.8 - asiakasyrityksen liiketoiminnalle? (Vähäinen/Kohtalainen/Merkittävä)
4.9 - alihankkijoiden ja muiden tuotannon yhteistyökumppaneiden liiketoiminnalle? (Vähäinen/Kohtalainen/Merkittävä)
4.10 - yrityksen omalle liiketoiminnalle? (Vähäinen/Kohtalainen/ Merkittävä)

5. Tuotekehityksen ja/tai palvelumuotoilun ongelmat

Onko IoT tieto käytössä - tai suunnittellaanko sen käyttöä - osana tuotekehitystä tai palvelumuotoilua?

Ei: siirry osioon 6.

Kyllä: **Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:**

5.1 - kehitettävän tuotteen/palvelun toiminnasta saadaan virheellinen kuva ja tuotetta kehitetään väärin (Kyllä/Ei)
5.2 - tuotekehityksen yhteistyökumppaneille toimitetaan virheellistä tietoa (Kyllä/Ei)
5.3 - uuden tuotteen hyväksyntä markkinoille perustuu virheellisiin tietohin (Kyllä/Ei)
5.4 - markkinoilla olevan tuotteen toiminnan/laadun ongelmia ei havaita eikä niihin puututa (Kyllä/Ei)
5.5 - markkinoilla olevan tuotteen toiminnasta saadaan virheellinen kuva ja tuotetta kehitetään turhaan/väärin (Kyllä/Ei)

Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa:

5.5 - tuotekehityksen yhteistyökumppaneiden liiketoiminnalle? (Vähäinen/ Kohtalainen/Merkittävä)
5.6 - yrityksen omalle liiketoiminnalle? (Vähäinen/Kohtalainen/Merkittävä)

6. IoT tiedon käsittelyvirheistä aiheutuvat yleiset ongelmat

Voiko IoT tietojen väärä käsittely johtaa sanktioihin tai yrityskuvan kannalta merkittäviin haittoihin?
Voivatko ongelmat IoT tiedon keräämisessä ja käsittelyssä johtaa siihen, että:

6.1 - yritys rikkoo EU:n tietosuoja-asetusta käsittelemällä henkilöitä koskevia tietoja väärin (Kyllä/Ei)
6.2 - yritys menettää laatuakreditoinnin puutteelliseksi havaitun tietoturvan vuoksi (Kyllä/Ei)
6.3 - tietoturvan puutteiden käsittely julkisuudessa vaikuttaa yrityksen, tuotteen ja/tai palvelun maineeseen (Kyllä/Ei)
6.4 - yritys joutuu maksamaan hakkereille välttääkseen negatiivisen julkisuuden (Kyllä/Ei)
6.5 - kilpailijat saavat käsiinsä tuotteen toimintaa koskevia tietoja ja käyttävät niitä oman tuotteensa kehittämiseen (Kyllä/Ei)
6.6 - kilpailijat saavat käsiinsä tuotteen toimintaa koskevia tietoja ja käyttävät niitä tarjouskilpailuissa (Kyllä/Ei)
6.7 - yritykselle aiheutuu muu ongelmallinen tilanne, mikä:_____
6.8. Mikäli ongelmatilanne realisoituu, kuinka merkittävänä pidät haittaa:
6.8.1. asiakasyritysten liiketoiminnalle? (Vähäinen/Kohtalainen/ Merkittävä)

6.8.2. yhteistyökumppaneiden liiketoiminnalle? (Vähäinen/ Kohtalainen/ Merkittävä)
6.8.3. yrityksen omalle liiketoiminnalle? (Vähäinen/Kohtalainen/ Merkittävä)

C. YLEISET YHTEENVETÄVÄT KYSYMYKSET

- Mitkä ovat nähdäksesi suurimmat liiketoiminnan riskit nykyisestä ja suunnitellusta IoT käytöstä?

- Mitä toimenpiteitä tulisi tehdä, että keskeisten riskien todennäköisyys tai niistä aiheutuva haitta saadaan mahdollisimman pieneksi?

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-4029-4
ISSN 1239-1891