Sadetta Postareff

KYBERTURVALLISUUDEN TEHOKKAAMPI HYÖDYNTÄMINEN ORGANISAATIOIDEN JATKUVUUDENHALLINNASSA NYT JA HUOMENNA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Postareff, Sadetta
Kyberturvallisuuden tehokkaampi hyödyntäminen organisaatioiden jatkuvuudenhallinnassa nyt ja huomenna
Jyväskylä: Jyväskylän yliopisto, 2024, 104 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Jatkuvuudenhallinta organisaatioissa on kaiken toiminnan perusedellytyksiä. Ilman sitä toimijat eivät ei pysty toipumaan niiden liiketoimintaa merkittävästi häiritsevistä, tai kokonaan keskeyttävistä tapahtumista riittävän tehokkaasti ja nopeasti. Jatkuvasti ja nopeasti digitalisoituvassa yhteiskunnassa organisaatiot eivät voi enää toimia kybermaailman ulkopuolella, ja näin ollen kyberuhat muodostavat näille koko ajan merkityksellisemmän uhkakentän. Siksi kyberturvallisuuden merkitys jatkuvuudenhallinnan osana kasvaa jatkuvasti ja myös nousevien uhkien tunnistaminen on entistä kriittisempää.

Organisaatiokenttä on hyvin moninainen ja hajautunut niin toimijoiden koon kuin resurssienkin puolelta, joten myös varautumisen käytänteet ja toimintatavat vaihtelevat tällä puolella laajasti. Lainsäädännön, standardien ja auditointikriteeristöjen, viranomaistoimintaa ohjaavien vaatimusten ja asiantuntijapalautteiden avulla haetaan parhaita käytänteitä, jotka toimisivat erikokoisissa organisaatioissa toimialasta riippumatta.

Tutkimuksessa selvitetään teoreettisen tiedon, kirjallisuuskatsauksen, sekä empiirisen tutkimuksen keinoin kyselyiden ja haastatteluiden avulla mitkä ovat merkittävimpiä tämänhetkisiä ja nousevia kyberuhkia, miten hyvin kyberturvallisuus on huomioitu ja tunnistettu tällä hetkellä osana organisaatioiden jatkuvuudenhallintaa, sekä mitä keinoja näiden osa-alueiden vuorovaikutuksen parantamiseen ja tehostamiseen voidaan tunnistaa ja kehittää jatkoa ajatellen ennakoivasti, minimoiden toiminnan jatkuvuuteen vaikuttavia kyberuhkia.

Tutkimuksen tarkoituksena on tuottaa katsaus organisaatioiden jatkuvuutta vaarantaviin kyberuhkiin nyt, sekä ennakoivasti tulevaisuuden trendit huomioiden. Samalla pyritään tarjoamaan erikokoisiin toimintaympäristöihin soveltuvaa tietoa kyberturvallisuuden keinojen tehokkaammasta hyödyntämisestä jatkuvuudenhallinnan osana.

Asiasanat: kyberuhat, kyberturvallisuus, jatkuvuus, jatkuvuudenhallinta, organisaatiot, nousevat teknologiat, kybertrendit

ABSTRACT

Postareff, Sadetta
Effective use of cybersecurity in business continuity management in organizations
Jyväskylä: University of Jyväskylä, 2024, 104 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

Business continuity management is a prerequisite for all operations. Without it, organizations won´t be able to recover effectively enough from incidents that disrupt or stop their businesses. In the continuously and rapidly digitalizing world, actors cannot operate outside of cyberspace anymore, and therefore, cyber threats compose an increasingly significant threat environment for organizations. Consequently, the meaning of cybersecurity as a part of business continuity management is constantly growing.

The organization domains are very multifaceted and diverse, so the policies and ways of working also differ extensively. In the research, we look for best practices from critical infrastructure actors and authorities, as well as from information security and business continuity standards to provide working solutions suitable for variable organizations.

By using the theoretical framework and literature review, as well as empirical research via questionnaires and interviews the research examines how well cybersecurity is currently part of the business continuity management in organizations, and what means can be recognized to improve and enhance the interaction between these areas in the future to minimize the cyber threats compromising organization´s business continuity.

This research aims to provide information on current and trending cyber threats that impact business continuity in diverse company organizations. At the same time, it aims to more effectively use cybersecurity as a tool and means of business continuity management. This is performed by examining the current situation in companies, future trends and requirements, and, based on these findings, providing solutions for improvement.

Keywords: cyber threats, cybersecurity, business continuity, business continuity management, BCM, organizations, emerging technologies, cyber trends

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Organisaatioiden toimintaympäristöt kehittyvät koko ajan riippuvaisemmiksi informaatio- ja kyberympäristöistä. On vaikeaa kuvitella enää toimijoita, jotka pystyisivät välttämään digitalisaatiota, sillä suurin osa on integroinut digitaalitekniikan osaksi toimintojaan, puhutaan sitten sisällöistä, kanavista tai transaktioista (Neittaanmäki ym., 2021, s. 11), tai kommunikaatiosta, toiminnanohjauksesta, tuotekehityksestä, tai esimerkiksi tuotteiden valmistuksesta. Tätä kautta kyberturvallisuus on koko ajan tärkeämmässä roolissa organisaatioiden turvallisuuden hallinnassa, ja tämä trendi tulee jatkumaan tulevaisuudessa niin teknologioiden jatkuvan kehityksen, kuin digitaalisen transformaation myötä.

Jatkuvuudenhallinta taas on organisaatioiden toiminnan perusedellytys, jossa on kyse kriittisiin toimintoihin ja ydinprosesseihin kohdistuvien riskien tunnistamisesta, priorisoinnista ja sitä kautta toimintaedellytysten turvaamisesta eri keinoin. Ilman jatkuvuudenhallintaa toipuminen sen toimintaan kohdistuvista vakavista häiriötilanteista, tai sen keskeyttävistä tapahtumista riittävän tehokkaasti, nopeasti, ja vahingot hyväksyttävälle tasolle rajaten. Jatkuvuudenhallinnalla huolehditaan siis organisaation ja sen kumppaneiden toimintaedellytyksistä (Huoltovarmuuskeskus [HVK], ei pvm.).

Molemmat, sekä kyberturvallisuus että jatkuvuudenhallinta ovat siis toimintaedellytysten varmistamiseksi kriittisiä. Lähes poikkeuksetta näiden arvo omina osa-alueinaan toiminnalle on myös tunnistettu ainakin jollain tasolla. Painotus näiden välillä, sekä syy-yhteyksien ja keskinäisen merkittävyyden ymmärtäminen vaihtelevat kuitenkin huomattavasti organisaatioittain.

Tutkielmassa pyritään tunnistamaan merkittävimpiä kyberuhkia organisaatioille nyt ja tulevaisuudessa. Lisäksi etsitään keinoja, joilla erikokoiset toimijat voivat suojata toimintaedellytyksiään ja tärkeimpiä omaisuuseriään kyberturvallisuuden keinojen priorisoimisella, tehokkaammalla huomioimisella, sekä yhdistämisellä jatkuvuudenhallinnan prosesseihin kehittäen riskinhallintaa, resilienssiä, palautumiskykyä, sekä varautumista vakaviin häiriötilanteisiin.

Tutkielmassa keskitytään selvittämään kirjallisuuskatsauksella saatavilla olevan tieteellisen materiaalin, sekä asiantuntijatiedon avulla mitkä ovat merkittävimpiä kybermaailman uhkia ja mahdollisuuksia organisaatioille nyt ja

lähitulevaisuudessa. Lisäksi tarkastellaan kyberturvallisuutta osana jatkuvuudenhallintaa ja sen prosesseja organisaatioissa, jotta voitaisiin tunnistaa, miten hyvin kyberturvallisuus on huomioitu osana varautumista. Tämän avulla pyritään arvioimaan mitä organisaatioiden tulisi toiminnassaan jatkuvuudenhallinnan näkökulmasta huomioida, parantaa ja mihin tulisi ennakoivasti keskittyä.

Tutkimusaihe koetaan tärkeäksi, koska kyberturvallisuuden merkittävyys kasvaa koko ajan muuttuvassa maailmassa, jossa uhkakuvat kehittyvät jatkuvasti, mutta ei ole selkeää, miten hyvin ja tehokkaasti organisaatiot ovat varautuneet tähän varmistaakseen toimintojensa jatkuvuuden. Koska on kuitenkin oletettavaa, että käytännöt ja resurssit vaihtelevat koosta, toimialasta ja resursseista riippuen, koetaan tärkeäksi tarjota ymmärrystä merkittävimmistä nykyisistä ja nousevista uhkista jotta nämä voivat suojata toimintaedellytyksiään mahdollisimman tehokkaasti priorisoiden.

Tutkimus jakautuu teoreettiseen osuuteen, jossa selvitetään jatkuvuudenhallintaa ja kyberturvallisuutta organisaatioissa, sekä kyberuhkia nyt ja tulevaisuudessa kirjallisuuskatsauksen sekä asiantuntijalähteiden avulla. Empiirisen tutkimuksen osiossa organisaatioiden tilannetta, kehitysehdotuksia sekä nykyisiä ja tulevaisuuden uhkia selvitetään kyselyn ja haastatteluiden avulla. Näiden tuloksia verrataan teoreettisen osion huomioihin ja löydöksiin etsien keinoja tutkimusongelmaan, eli miten jatkuvuudenhallintaa voitaisiin parantaa tehostamalla kyberturvallisuutta toiminnassa.

Tutkielman tuloksena halutaan saada organisaatioiden käyttöön käsitys siitä, mitkä ovat merkittävimmät uhat organisaatioille nyt ja lähitulevaisuudessa, sekä miten kyberturvallisuus tulisi huomioida osana jatkuvuudenhallintaa mahdollisimman tehokkaasti ja toimenpiteitä priorisoiden, jotta toiminnan jatkuvuuteen liittyviä riskejä voitaisiin minimoida.

1.1 Tutkimuksen tausta ja tavoitteet

Tutkimuksen tarkoituksena on selvittää mikä on organisaatioihin kohdistuvaa uhkakenttä nyt ja lähitulevaisuudessa kybermaailmassa, miten teknologinen kehitys voi vaikuttaa jatkuvuudenhallintaan ja miten tämä tulisi huomioida organisaatioissa. Halutaan käsitellä ja hahmottaa myös sitä mitä on tulossa, ei vain nykytilannetta, sekä auttaa organisaatioita priorisoimaan resurssejaan jatkuvuudenhallintansa tehostamiseksi. Tutkimuksen kiinnostavuus kiteytyy nykytilanteen ja tulevien trendien ymmärtämiseen, sekä siihen miten jatkuvuudenhallintaa voidaan parantaa nämä asiat ymmärtämällä, auttaen toimijoita kohdistamaan resurssejaan mahdollisimman tehokkaasti.

1.2 Tutkimuskysymykset ja aiheen rajaus

Tutkimuksen päätutkimuskysymys on:

Miten merkittävimmät ja nousevat kyberuhat tunnistetaan ja huomioidaan osana jatkuvuudenhallintaa ja miten näihin varautumista voitaisiin tehostaa?

Lisäksi tutkimuksella on seuraavat alatutkimuskysymykset:

a. Mitkä ovat merkittävimpiä kyberuhkia organisaatioille nyt ja tulevaisuudessa?
b. Onko kybermaailman aiheuttamat uhat tunnistettu riittävän hyvin organisaatioissa ja turvaavat toimenpiteet toteutettu?
c. Mikä on organisaatioiden arvioitu kyky vastata jatkuvuutta vaarantaviin kyberuhkiin?
d. Miten kyberturvallisuuden avulla voidaan tehostaa jatkuvuudenhallintaa nykyisestään organisaatioissa?

Tutkimuskohde rajataan tässä tutkielmassa erilaisiin organisaatioihin, sekä keskitytään jatkuvuuteen vaikuttaviin uhkiin, jotka kohdistuvat organisaatioihin ja joihin voidaan vaikuttaa kyberturvallisuuden keinoin.

Tutkimuksen ulkopuolelle rajataan yksilöt, sekä erilaiset epäviralliset ryhmät, joilla ei ole selkeää organisaation määritelmän täyttävää rakennetta, sekä kansallinen ja valtiollinen turvallisuus teemana, vaikka kriittiseen infrastruktuuriin liittyviä organisaatioita voikin olla osana tutkimusta. Tutkimuksen kirjallisuuskatsauksessa käytetyissä asiantuntijamateriaaleissa ei ole rajattu toimijoita maantieteellisesti, mutta lainsäädännön ja standardien osalta keskitytään Suomen ja EU:n alueella käytettäviin säädöksiin ja materiaaleihin. Empiirisen osuuden osalta (kysely, haastattelut) tutkimus rajataan tutkimuskielen vuoksi Suomea ymmärtäviin asiantuntijoihin. Jatkuvuudenhallinnan osalta tutkimuksen ulkopuolelle jätetään valmiussuunnittelu ja poikkeusolot. Kyberturvallisuuden osalta ulkopuolelle rajataan pääasiallisesti muut digitaalista turvallisuutta tukevat osa-alueet, kuten toiminnan turvallisuus, tietoturvallisuus, tietosuoja ja fyysinen turvallisuus. Näitä voidaan sivuta aihealuetta tukevina aspekteina, mutta niihin ei paneuduta syvällisesti.

1.3 Tutkielman rakenne

Johdannossa kuvataan tutkielman taustaa, tarkoitusta ja tarvetta tutkimukselle, määritetään tutkimuskysymykset ja aiheen rajaukset, sekä avataan käytettyjä käsitteitä.

Luvut toisesta viidenteen (2–5) keskittyvät aihealueen teoreettiseen tarkasteluun ja tiedon keräämiseen kirjallisuuskatsauksen avulla eri näkökulmista.

Toisessa luvussa tarkastellaan jatkuvuudenhallintaa yleisesti käsitteenä, mitä se tarkoittaa, sekä sen lisäksi jatkuvuudenhallinnan toteuttamisen keinoja

organisaatioissa. Kolmannessa luvussa tarkastellaan ensin kyberturvallisuutta käsitteenä, kybermaailman tämänhetkistä tilaa ja merkittävimpiä uhkia, sekä mitkä tekijät ohjaavat kyberturvallisuuden hallintaa. Neljännessä luvussa käsitellään vielä jatkuvuudenhallintaa ja kyberturvallisuutta ohjaavia yhteisiä tekijöitä ja tarkastellaan näiden jakamia hallintakeinoja. luvussa tarkastellaan kyberturvallisuusuhkien trendejä tulevaisuudessa, sekä kehittyvän teknologian vaikutusta organisaatioiden kyberuhkiin. Kuudes kappale käsittelee tutkimuksen teoreettista viitekehystä ja sen menetelmiä niin kirjallisuuskatsauksen kuin empiirisen tutkimuksen osalta, sekä määrittelee ja kuvaa empiirisen tutkimusosuuden aineistonkeruumenetelmät. Viimeisessä, seitsemännessä luvussa analysoidaan tutkimuksen löydöksiä, merkittävyyttä ja hyödyllisyyttä, sekä tehdään yhteenveto ja omaa pohdintaa tutkielmaa koskien. Kappaleessa arvioidaan myös tutkimuksen luotettavuutta, sekä tarvetta mahdolliselle jatkotutkimukselle ja sen suunnalle.

1.4 Tutkimuksen keskeiset käsitteet

Tutkielman keskeinen käsitteistö liittyy jatkuvuudenhallintaan, kybermaailman ympärille, sekä näihin liittyvää lainsäädäntöön, standardeihin ja alan vakiintuneeseen termistöön. Seuraavissa kappaleissa 1.4.1 ja 1.4.2 tarkennetaan tutkimuksessa käytettyjä termejä ja käsitteitä jaotellen nämä jatkuvuudenhallinnan ja kyberturvallisuuden käsitteisiin.

Käsitteiden osalta on huomioitava, että vaikka termejä ”tietoturvallisuus” ja ”kyberturvallisuus” käytetään usein rinnakkain, niin tietoturvallisuudella tarkoitetaan kaikkia toimenpiteitä ja keinoja, joilla suojataan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kun taas kyberturvallisuus keskittyy sähköisen ja verkottuneen toimintaympäristön turvaamiseen (Turvallisuuskomitea, 2018, s. 15, 22). Näille kattotermi on Digi- ja väestötietoviraston (DVV) mukaan ”digitaalinen turvallisuus” joka kattaa niin jatkuvuudenhallinnan, kuin kyber- ja tietoturvallisuudenkin (Digi- ja Väestötietovirasto [DVV], 2023a).

1.4.1 Jatkuvuudenhallintaan liittyvät termit ja käsitteet:

- Jatkuvuudenhallinnalla tarkoitetaan toiminnan jatkuvuuden varmistamista suunnittelemalla toimenpiteet ja prosessit häiriötilanteiden ennaltaehkäisemiseksi, niihin varautumiseksi kuin niistä palautumiseksi resilienssiä kasvattamalla (Sanastokeskus, 2018a.).
- Jatkuvuussuunnittelu tarkoittaa niitä toimia ja keinoja, joilla häiriötilanteiden vaikutuksia pyritään pienentämään ja lyhentämään. Jatkuvuussuunnittelu toteuttaa jatkuvuudenhallinnan kokonaiskehystä ja sisältää sekä jatkuvuus- että toipumissuunnitelmat (Valtiovarainministeriö [VM], 2016a).

- Jatkuvuussuunnitelmat ovat nimensä mukaisesti suunnitelmia, joiden avulla toiminta turvataan häiriötilanteiden aikana ja niiden jälkeen. Suunnitelmissa katetaan tarvittavalla tasolla toimijat, resurssit, palvelut ja toimenpiteet (Sanastokeskus, 2016a).
- Liiketoiminnan vaikutusanalyysi (engl. BIA, Business Impact Analysis), jolla tunnistetaan ja priorisoidaan organisaation kriittisimmät toiminnot, sekä näiden väliset riippuvuudet. Tämän lisäksi tunnistetaan näihin vaikuttavat haitalliset tekijät (VM, 2016a).
- MBCO (engl. Minimum Business Continuity Objective) on alin hyväksyttävä taso, jolle toiminnot voivat häiriön vuoksi tippua ilman, että liiketoiminnan keskeiset tavoitteet menetetään (Spedan, 2019).
- MTPD (engl. Maximum Tolerable Period of Disruption) on maksimiaika minkä toiminnot voivat olla minimitavoiterajojen alapuolella ennen kuin ne voivat aiheuttaa peruuttamatonta vahinkoa liiketoiminnalle (Spedan, 2019).
- RPO (engl. Recovery Point Objective) eli toipumispiste, joka määrittelee minimivaatimukset tilalle johon, toiminnot tulee saada palautettua häiriötilanteen jälkeen. Se kuvaa myös miten paljon dataa voidaan menettää vaikuttaen suoraan varmuuskopioinnin taajuuteen (VM, 2016a).
- RTO (engl. Recovery Time Objective) eli toipumisaika, jolla määritellään toiminnon tavoiteltu toipumisaika (VM, 2016a).
- Toipumissuunnitelmat ovat osa jatkuvuussuunnitelmia, joissa kuvataan toimenpiteet häiriöistä palautumiseen. Useimmiten toipumissuunnitelmat liittyvät IT-järjestelmiin ja tietotekniseen toipumiseen (Sanastokeskus, 2016b).

1.4.2 Kyberturvallisuuteen liittyvät termit ja käsitteet:

- DoS ja DDoS: Palvelunestohyökkäys (Denial of Service attack, DoS) ja hajautettu palvelunestohyökkäys (Distributed Denial of Service attack, DDoS) ovat verkkohyökkäyksen muotoja, joilla pyritään lamauttamaan palvelu tai tietojärjestelmä. Hyökkäys voi tulla yhdestä osoitteesta (DoS), tai esim. bottiverkon kautta useista lähteistä yhtä aikaa (DDoS). (Sanastokeskus, 2014).
- Digitaalinen turvallisuus kattaa johtamisen ja riskienhallinnan, jatkuvuudenhallinnan, tieto- ja kyberturvallisuuden, sekä tietosuojan. (DVV, 2023a)
- Digitalisaatio (Neittaanmäki ym., 2021, s. 12)
- Haktivisti on hakkeri, jolla on aatteellinen motiivi. (Sanastokeskus, 2004)
- ICT (engl. Information and Communication Technology) tarkoittaa tieto- ja viestintäteknologiaa (Sanastokeskus, 2010).
- IoT (engl. Internet of Things) eli esineiden internet tarkoittaa laitteita, joissa internetiä käytetään niiden ohjaamiseen ja hallintaan (Sanastokeskus, 2017).
- Kybertoimintaympäristö (myös kybermaailma/kyberfyysinen maailma) määritellään digitaalisista tietojärjestelmistä muodostuviksi

toimintaympäristöiksi, joille on tunnusomaista datan kaikinpuolinen käsittely elektronisin keinoin sisältäen myös fyysiset rakenteet. (Turvallisuuskomitea, 2018, 21).

- Kyberturvallisuudella haetaan kybertoimintaympäristön luotettavuutta toimenpiteillä, joilla voidaan hallita ja sietää kyberuhkia ja niiden vaikutuksia (Turvallisuuskomitea, 2018, 25). Kyberturvallisuus on usein (tieto)turvallisuuden osa-alue. Kyberturvallisuus keskittyy tiedon ja tietojärjestelmien, sekä laitteiden turvallisuuden takaamiseen verkkoympäristössä (F-Secure, ei pvm.)
- Kyberuhkilla tarkoitetaan kybertoimintaympäristöön kohdistuvia haitallisia tapahtumia, jotka voivat vaarantaa siitä riippuvaiset toiminnot (Turvallisuuskomitea, 2018, s. 25)
- Lohkoketjut (engl. Blockchain, BCT) on hajautettu, kehittyvä datakokonaisuus, jossa tapahtumat ovat aina aikajärjestyksessä, vahvistettuja, ja jälkikäteen muuttamattomissa. (Sanastokeskus, 2018b)
- Massadata (iso data, big data) tarkoittaa niin massiivisia ja nopeasti kasvavia sekä muuttuvia tietokokonaisuuksia, että niitä on vaikea käsitellä nykyisillä tietojenkäsittelysovelluksilla (Sanastokeskus, 2013)
- Nollapäivähaavoittuvuus on tietoturvahaavoittuvuus, josta ohjelman kehittäjät tulevat tietoiseksi vasta kun tieto julkaistaan, eli kehittäjille jää nolla päivää aikaa haavoittuvuuden poistamiseen (Sanastokeskus, 2018c).
- OT (Operational technology) tarkoittaa tuotantoympäristöjen IT-järjestelmiä, teknologiaa ja verkkoja joilla hallitaan tuotantoympäristöjen laitteistoja ja niiden toimintaa (Yassine, 2021).
- Standardit ovat erilaisia yhteisiin toimintatapoihin, hyviin käytäntöihin ja aihealueeseen liittyviin vaatimuksiin sekä ratkaisuihin kohdistuvia julkaisuja, joilla organisaatiot ja toimijat voivat varmistaa vaatimuksenmukaisuuttaan esimerkiksi tuotteiden, palvelujen, tai järjestelmien toimintaan liittyen (SFS Suomen Standardit [SFS], ei pvm.). Tutkielmassa käytettyjä standardeja ovat mm. tietoturvallisuuden standardisarja ISO/IEC 27000 -sarja (ISMS, ei pvm.), sekä turvallisuuden ja kriisinkestävyyden standardi ISO/IEC 22301 (SFS 22301:2019, 2019).
- Tekoäly (AI, Artificial Intelligence). Tekoäly jakautuu perinteiseen ja generatiiviseen tekoälyyn. Tekoäly terminä tarkoittaa ”*ohjelmaa, joka jäljittelee ihmiselle tyypillisiä älykkyyttä vaativia toimintoja*” (Sanastokeskus, 2022)
- Tietoturvaloukkaus (engl. data breach) tarkoittaa oikeudetonta puuttumista tietoon tai tietojärjestelmään erilaisia hyökkäysvektoreita käyttäen, kuten salasanojen tai tunnusten väärinkäytöllä, haittaohjelmilla, palvelunestohyökkäyksillä (Dos/DDos), tai tietomurroilla (Sanastokeskus, 2018d).
- Tietoallas (Data lake) on arkkitehtuuriratkaisu, joka perustuu teknologisten ratkaisuiden hyödyntämiseen isojen tietomassojen käsittelyssä (Neittaanmäki ym., 2021, s. 77-85)

2 JATKUVUUDENHALLINTA ORGANISAATIOISSA

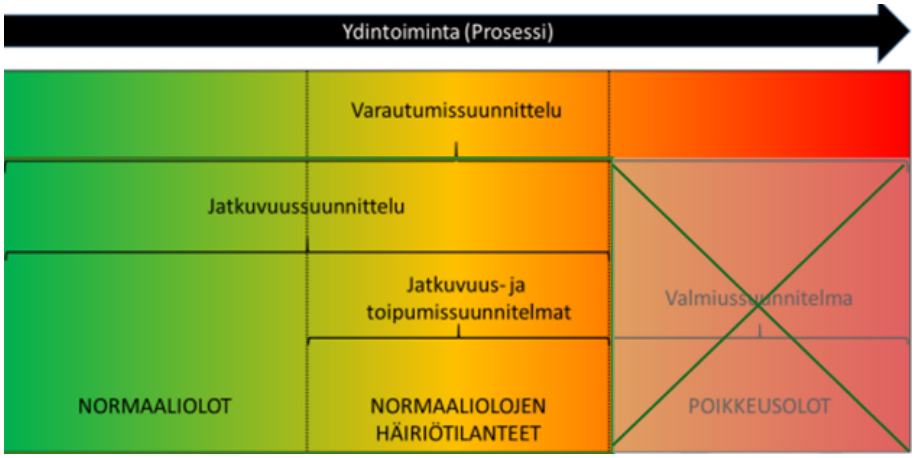
Kappaleessa käydään läpi mitä jatkuvuudenhallinta tarkoittaa käsitteenä, sen merkitystä organisaatioille, sekä siihen liittyviä osa-alueita ja prosesseja.

2.1 Jatkuvuudenhallinta käsitteenä

Turvallisuuskomitean Kyberturvallisuuden sanastossa, sekä Huoltovarmuuskeskuksen sivuilla jatkuvuudenhallintaa kuvataan organisaatioiden huoltovarmuutta parantavaksi prosessiksi, jonka avulla tunnistetaan toiminnan uhat, riskit, häiriötilanteet sekä riippuvuudet, ja voidaan arvioida niiden vaikutukset niin organisaatioissa kuin näiden toimijaverkostossakin. Tämän lisäksi voidaan luoda ja toteuttaa menettelytavat erilaisten toimintaa uhkaavien häiriötilanteiden varalle, sekä suojata toiminnan jatkuvuus, toiminnan intressit ja arvontuotto kaikissa olosuhteissa (HVK, ei pvm.; Turvallisuuskomitea, 2018).

Kyberturvallisuuskeskuksen mukaan *"Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla."* (Turvallisuuskomitea, 2018).
Näiden mukaan jatkuvuudenhallinta on johdon tuella tapahtuvaa, pääsääntöisesti omaehtoista toimintaa organisaatioissa näiden resilienssin kasvattamiseksi, mutta osan tulee huomioida lakien asettamat vaatimukset (HVK, ei pvm.; Turvallisuuskomitea, 2018).

Jatkuvuudenhallinta on kokonaisuutena varautumissuunnittelua, joka jakautuu normaaliolojen häiriötilainteisiin keskittyvään jatkuvuussuunnitteluun, sekä valmiussuunnitteluun, joka käsittelee poikkeusolojen häiriötilanteita. Tässä tutkimuksessa keskitytään normaaliolojen prosesseihin jättäen poikkeusolojen prosessit ulkopuolelle kuten selvennetään Valtiovarainministeriön (2016a, s. 23) käyttämässä Iivarin & Laaksosen kuvassa (2009) (KUVIO 1).



KUVIO 1: Jatkuvuudenhallinnan käsitteet. Iivari & Laaksonen, 2009.

Tämän lisäksi organisaatioiden tulee tunnistaa sidosryhmänsä ja näiden tarpeet sekä vaatimukset. Sidosryhmäkenttä on hyvin monimuotoinen, ja kaikkien osapuolten tunnistaminen voi olla haastavaa ja vaihdella organisaatioittain. Valtiovarainministeriön (2016a, s. 29) kuva antaa hyvän esimerkin kentän laajuudesta (KUVIO 2).

KUVIO 2: Esimerkki sidosryhmistä. Valtiovarainministeriö, 2016a.

Organisaation jatkuvuudenhallinnan vastuiden määrittäminen on samalla tavoin tärkeää kuin turvallisuuden hallinnassakin, kun sidosryhmät ja toimijat on tunnistettu. Johdon tulee luoda edellytykset jatkuvuudenhallinnan onnistumiselle (tavoitteet, linjaukset, resurssit, budjetointi jne.) sekä seurata tavoitteiden täyttymistä. Muu organisaatio tulee määrittää toimintojen, prosessien, palvelujen ja tietojärjestelmäomistajuuksien mukaan, ja tämän lisäksi organisaation pitää tunnistaa ja vastuuttaa sisäisten ja ulkoisten toimijoidensa osalta tarpeelliset tahot kokonaisvaltaisen jatkuvuudenhallinnan takaamiseksi (VM 2016a).

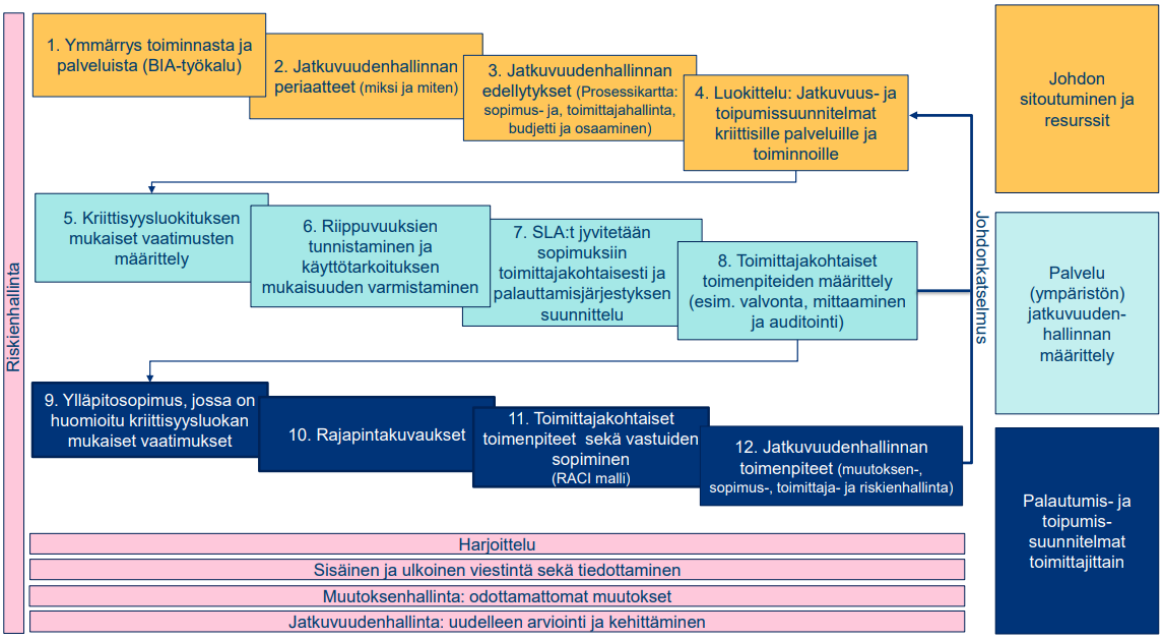
Toiminnan tulee olla dokumentoitua ja jatkuvaan parantamiseen pyrkivää. Tällä tarkoitetaan niin prosesseja, dokumentaatiota, riskienhallintaa, muutoshallintaa, viestintää, kuin osaamista ja koulutustakin. Jatkuvuudenhallinta on jatkuvaa uudelleenarviointia ja toiminnan kehittämistä. Näissä tärkeinä apukeinoina ovat mm. sisäiset ja ulkoiset auditoinnit, sekä toiminnan testaaminen ja harjoittelu. Seuraavassa kappaleessa käsitellään tarkemmin toimintoja ja dokumentaatiota, jolla jatkuvuudenhallintaa suoritetaan.

2.2 Jatkuvuussuunnittelu organisaatioissa

Jatkuvuudenhallinta organisaatiossa on siis varautumista vakaviin häiriötilanteisiin, jotka voivat uhata liiketoiminnan jatkuvuutta, toipumista hyväksyttävissä raameissa näistä häiriötilanteista, sekä resilienssin (kriisinkestävyyden)

kasvattamista. Jatkuvuussuunnittelu sisältävää ja tarkentaa keinoja jatkuvuudenhallinnan takaamiseksi.

Toteutettavia toimintoja organisaatioissa tarkasteltiin Digi- ja Väestötietoviraston jatkuvuudenhallinnan yhteisen mallin kautta (KUVIO 3). Samoihin asioihin ottaa kantaa myös mm. Turvallisuuden ja kriisinkestävyyden standardi SFS-EN ISO 22301:2019 (2019).



KUVIO 3: Yhteinen malli jatkuvuudenhallintaan (DVV, 2024)

Yllä kuvataan jatkuvuudenhallinnan kokonaismallia kattavasti, määrittäen mitä kaikkea organisaatioiden tulee ottaa huomioon. Tutkimuksen teoreettisen osuuden kannalta katsottiin tarpeelliseksi avata osittain kuvan kohtia. Osiot jaettiin alempana kolmeen kappaleeseen kuvan mukaisesti.

Riskienhallinta näkyy kuvassa sivupalkkina tarkoittaen, että se koskee kaikkea jatkuvuudenhallintaan liittyvää. Uhkien tunnistaminen ja riskienhallinta ovat prosesseja, joita ei voi erottaa vain tiettyyn aihealueeseen kohdistettaviksi. Riskienhallinnan tulee olla jatkuvaa ja systemaattista (Lehto, 2023, s. 140). Samoin alapalkeissa näkyvät harjoittelu, viestintä ja tiedottaminen, muutoksenhallinta ja jatkuva uudelleenarviointi ja kehittäminen ovat kaikkiin osa-alueisiin kohdistuvia toimintoja.

2.2.1 Johdon sitoutuminen ja resurssit

Johdon tulee sitoutua sekä mahdollistaa jatkuvuudenhallinta, ja toiminnan tulee linkittyä liiketoiminnan strategiaan. Organisaation tulee tuntea sisäinen ja ulkoinen toimintaympäristönsä, huolehtia tavoitteiden määrittelystä ja henkilöstön vastuuttamisesta, sekä tunnistaa ja priorisoida ydinprosessit ja toiminnot

kriittisyyden perusteella. Myös näihin liittyvät palvelut, prosessit, järjestelmät ja riippuvuussuhteet tulee tunnistaa (VM 2016a, s. 30-32).

Johdolla tulee olla ymmärrys toiminnasta ja palveluista. Liiketoiminnan vaikutusanalyysin avulla kartoitetaan kriittisimmät toiminnot ja niiden riippuvuussuhteet. Malleja tämän luomiseen on useita, mutta vaikutusanalyysin tulee sisältää kriittisimmät toiminnot ja järjestelmät, näiden kriittisyysluokittelun toisiinsa nähden (=määritellään näiden käytettävyysluokitus sekä palvelutasovaatimus), niihin vaikuttavat haitalliset tekijät, sekä toimintojen riippuvuussuhteet toisiinsa (VM 2016a, s. 27-29).

Lisäksi varmistetaan jatkuvuudenhallinnan edellytykset myös dokumentaatiossa. Tämä kattaa mm. sopimushallinnan, budjetoinnin, organisaatiokaaviot, viestinnän ja vastuut, prosessikartat, muutoksenhallinnan prosessit, vuosikellon, sen miten toimittajahallintaa suoritetaan, sekä mitkä ovat vaatimukset ja linjaukset. Niin hallinnolliset kuin tekniset toimenpiteet tulisi dokumentoida (VM 2016a, s. 41-42).

Neljännen kohdan jatkuvuussuunnitelmat ja toipumissuunnitelmat ovat merkittävä osa varautumisen prosesseja. Näissä kuvataan erilaisista häiriötilanteista palautuminen sen mukaan mitä mm. liiketoiminnan vaikutusanalyysissa on tunnistettu ja määritetty, sekä periaatteissa kuvattu. Jatkuvuussuunnitelmat keskittyvät ydintoimintojen ylläpitoon siinä missä toipumissuunnitelmat kohdistuvat järjestelmiin ja verkkoon.

2.2.2 Palveluympäristön jatkuvuudenhallinnan määrittely

Organisaation tunnistettua ja määritettyä toimintonsa yllä olevan kuvan (KUVIO 3) mukaisesti varmistetaan tarkemmin hallinnan määrittelyä. Käytännössä tässä vaiheessa luodaan tunnistetuille toiminnoille jatkuvuus- ja toipumissuunnitelmat. Näissä pohjana toimii liiketoiminnan vaikutusanalyysi sekä johdon linjaukset. Vaikutusanalyysin avulla määritellään yleensä hyväksyttävät RTO (Recovery Time Objective) joka linjaa tavoitellun toipumisajan, RPO (Recovery Point objective) joka määrittää toipumispisteen, eli tilan johon järjestelmät, tieto, tai toiminnot pitää saada palautettua mm. varmuuskopioinnin kautta (VM, 2016a, s. 24-25). Tämän lisäksi mm. jatkuvuudenhallinnan ja kriisinkestävyyden ISO -standardi antaa kaksi määritystä, jotka organisaation tulisi arvioida: MTPD (Maximum Tolerable Period of Disruption), eli maksimiaika, jonka kriittiset toiminnot voivat olla alhaalla, sekä MBCO (Minimum Business Continuity Objective) joka auttaa organisaatioita määrittämään minimitason jolle toiminnot saavat pudota häiriötilanteessa. (SFS-EN ISO 23301:2019, 2019). Yleensä tutkimuksissa vältetään lyhenteiden käyttöä, mutta yllä olevat termit ovat niin yleisesti käytettyjä ja jatkuvuudenhallintaan liitettyjä, että tehtiin ratkaisu ottaa ne mukaan.

Liiketoiminnan vaikutusanalyysin kautta on tunnistettu myös riippuvuussuhteet, ja tässä vaiheessa näiden tulisi kehittyä ohjaavaksi dokumentaatioksi, jolla jatkuvuudenhallintaa voidaan suorittaa. Tässä vaiheessa tulee mukaan selkeämmin myös toimittajahallinnan aspekti, sillä määritetyt toipumisajat tulee johtaa toimittajien kanssa tehtyihin sopimuksiin vasteaikavaatimuksina. Jos

toipumisaika sekä maksimiaika jonka toiminnot voivat olla alhaalla on määritelty tietylle tasolle, tulee varmistaa, että toimintoon vaikuttavien sidosryhmien ja toimitusketjujen sopimukset vastaavat näihin vaatimuksiin. Tässä yhteydessä tulee taas nostaa esiin toimitusketjuturvallisuuteen kohdistuvat uhat ja riskit, jotka pitää olla tunnistettu. On myös tunnistettava, miten toimittajia tulee valvoa, heidän suoriutumistaan mitata, sekä miten toimittaja-auditoinnit suoritetaan ja viedään sopimuksiin.

2.2.3 Palautumis- ja toipumissuunnitelmat toimittajittain

Viimeinen osa (KUVIO 3) kohdistuu jatkuvuudenhallinnan vastuuttamiseen ja vaatimiseen myös toimittajilta. Tässä DVV (2024) huomioi toimittajaketjun turvallisuutta organisaatioiden jatkuvuudenhallinnan kannalta.

Sopimuksiin tuli viedä organisaation kriittisyysluokittelun mukaiset vaatimukset, jotta ne ovat linjassa toipumisaikatavoitteiden kanssa. Tämä koskee ylläpitosopimuksia, mutta myös mitä tahansa palvelusopimuksia, joissa on tunnistettu toimittajavastuita, sekä yhteistä rajapintaa.

Vastuiden ja tehtävien toimenpiteiden tulee olla selkeästi kuvattu mm. vastuiden allokointimatriisissa (RACI-malli), joka kattaa myös toimittajat, ja organisaation pitää tunnistaa miten toimittajat liittyvät häiriötilanteista palautumiseen. Myös viestintäsuunnitelma tulee olla kuvattuna kattaen toimittajat (VM 2016a, s. 56-58)

2.3 Yhteenveto

Edellä läpikäytyjen prosessien ja tuotetun dokumentaation kautta organisaatio pystyy varmistamaan jo monin osin jatkuvuudenhallintaansa ja sen toimenpiteitä. Organisaation toimialasta ja resursseista on kiinni, miten mittavasti jatkuvuudenhallintaa pystytään toteuttamaan. Suppeammassakaan mittakaavassa yllä olevia kohtia ei saisi kokonaan ohittaa, mutta rajatuilla resursseilla priorisointi voi olla pakollista, ja lakien ja regulaatioiden täyttämiseen tähtäävää.

3 KYBERTURVALLISUUS ORGANISAATIOISSA

Luvussa käydään läpi kyberturvallisuus käsitteenä, sekä mitä se tarkoittaa organisaatioissa. Lisäksi tutkitaan mitkä ovat tämän hetken merkittävimmät organisaatioihin kohdistuvat kyberuhkat, sekä miten näiltä suojautumisessa tulisi huomioida.

3.1 Kyberturvallisuus käsitteenä

Kyberturvallisuus on tietoturvallisuuden osa-alue joka keskittyy datan ja tietojärjestelmien, sekä laitteiden turvallisuuteen verkkoympäristöissä. Se on joukko prosesseja, erilaisia teknologisia ratkaisuja, sekä parhaita käytäntöjä joilla voidaan suojautua digitaalisilta hyökkäyksiltä verkon kautta leviävien haittaohjelmien ja muiden kyberuhkien vaikutuksilta (F-Secure, ei pvm.; Turvallisuuskomitea, 2018; Taherdoost, 2022a). Osa-alue on Suomen uusimman vuoden 2024 Valtioneuvoston kanslian (VNK) julkaiseman Kyberturvallisuusstrategian mukaan äärimmäisen tärkeä osa kokonaisturvallisuuden mallia yhteiskunnassa jonka toimintaympäristöjä määrittävät muun muassa voimakas digitalisaation kiihtyminen sekä uusien teknologioiden kehitys, mutta myös muuttunut geopoliittinen tilanne (Valtioneuvoston kanslia [VNK], 2024, s. 9).

Organisaatioiden kyberturvallisuus muodostuu johdon tuella tapahtuvasta liiketoimintakriittisten ympäristöjen ja suojattavan omaisuuden tunnistamisesta, toimintaan kohdistuvien kyberuhkien kartoittamisesta ja ymmärtämisestä, riskienhallinnasta, sekä oikeiden suojaavien toimenpiteiden valinnasta edellä mainittuihin liittyen.

Kyberturvallisuutta ja tietoturvallisuutta, tai muitakaan turvallisuuden osa-alueita ei voi useinkaan erottaa kyber-fyysisessä maailmassa kokonaan toisistaan vaikka ne keskittyvätkin suojaamaan tietoa eri keinoin. Esimerkiksi tietoturvallisuudesta huolehditaan enenevässä määrin kyberturvallisuuden keinoin, ja fyysinen turvallisuus on erottamaton osa sekä tieto- että kyberturvallisuutta. Samoin ihmistekijä on aina mukana puhuttaessa turvallisuudesta tai siihen kohdistuvista uhkista. Tätä periaatetta toteuttavat muun muassa monet tietoturvallisuuden hallintamallin standardit joita käsitellään myöhemmin. Organisaatiotasolla uhat pitää pilkkoa huomattavan paljon pienempiin kokonaisuuksiin, jotta voidaan tunnistaa mitä mikäkin uhkakenttä sisältää. Näin tarkkaan jaotteluun ei voida tässä tutkimuksessa mennä, mutta tässä kappaleessa käsitellään asiat, jotka jokaisen organisaation tulisi huomioida kyberturvallisuutta rakentaessaan, niin merkittävimpien uhkien kuin suojaavien toimenpiteidenkin osalta. Samalla tämä kappale toimii teoreettisena vertailuosiona jatkon empiiriselle osuudelle, jossa tarkastellaan organisaatioiden nykytilanteita ja mahdollisia kehitysehdotuksia.

3.2 Organisaatioihin kohdistuvat kyberuhat nyt

Digitalisaatio muuttaa toimintaympäristöjä koko ajan enemmän jakamistalouteen ja globaaliin itsepalveluyhteiskuntaan painottuviksi. Tämä tarkoittaa, että palveluita tuotetaan pääosin digitaalisilla, globaaleilla palvelualustoilla, joissa myös tekoälyllä on koko ajan suurempi merkitys (Neittaanmäki ym., 2021, s. 26).

Tämän muutoksen kautta kybermaailma on koko ajan merkittävämpi osa organisaatioiden toimintaa, ja myös uhkakenttä laajenee koko ajan. Uhat voivat aina olla ulkoisia tai sisäisiä, erilaisten rikollisten toimijoiden vaihtelevin motiivein aiheuttamia (valtiollinen, rikollinen, vandalismi jne.) aiheuttamia, tai ei-tahallisia vahingoista ja tietämättömyydestä johtuvia, sekä esim. luonnonilmiöihin liittyviä (Lehto, 2023). Uhkakentän laajeneminen liittyy siihen, että siinä missä ennen hyökkäysten suorittamiseen tarvittiin vahvempaa tietoteknistä osaamista, niin nykyään hyökkäystyökalut ovat kehittyneet helpommin käytettäviksi, sekä erilaisia hyökkäyksiä voi ostaa suoraan verkosta. Myös kehittyvä teknologia mukaan lukien tekoäly tuo koko ajan enemmän hyökkäysvektoreita rikollisten repertuaariin, ja aiemmat hyökkäykset voidaan suorittaa tehokkaammin (Microsoft, 2024, s.83-93).

Kyberrikollisuuden kulujen maailmantaloudelle arvioitiin olleen vuonna 2020 5,5 biljoonaa euroa Euroopan unionin kyberturvallisuusviraston (ENISA) mukaan (2022) ja mm. IBM laskee vuosittaisessa raportissaan yrityksille aiheutuvan tietoturvaloukkauksista keskimäärin n. 4,1 miljoonan euron vahingot, Skandinavian keskiarvon ollessa n. 1,9 miljoonaa euroa (IBM, 2023, 9-12). Jo pelkästään näiden lukujen valossa taloudellista uhkaa voidaan pitää huomattavana.

Liiketoimintaan ja organisaatioihin kohdistuvat uhat ovat huomattavan monimuotoiset, eikä kaikkien luetteleminen ollut mielekästä, kun haluttiin keskittyä auttamaan organisaatioita tunnistamaan ja priorisoimaan suojaustoimenpiteitään toimintansa jatkuvuuden turvaamiseksi. Merkittävimpien kyberuhkien ja hyökkäysvektoreiden tunnistamiseen valittiin muutamia tunnettuja organisaatioita, jotka julkaisevat säännöllisesti kattavia raportteja joiden avulla voitiin pyrkiä tunnistamaan tämän hetken trendejä.

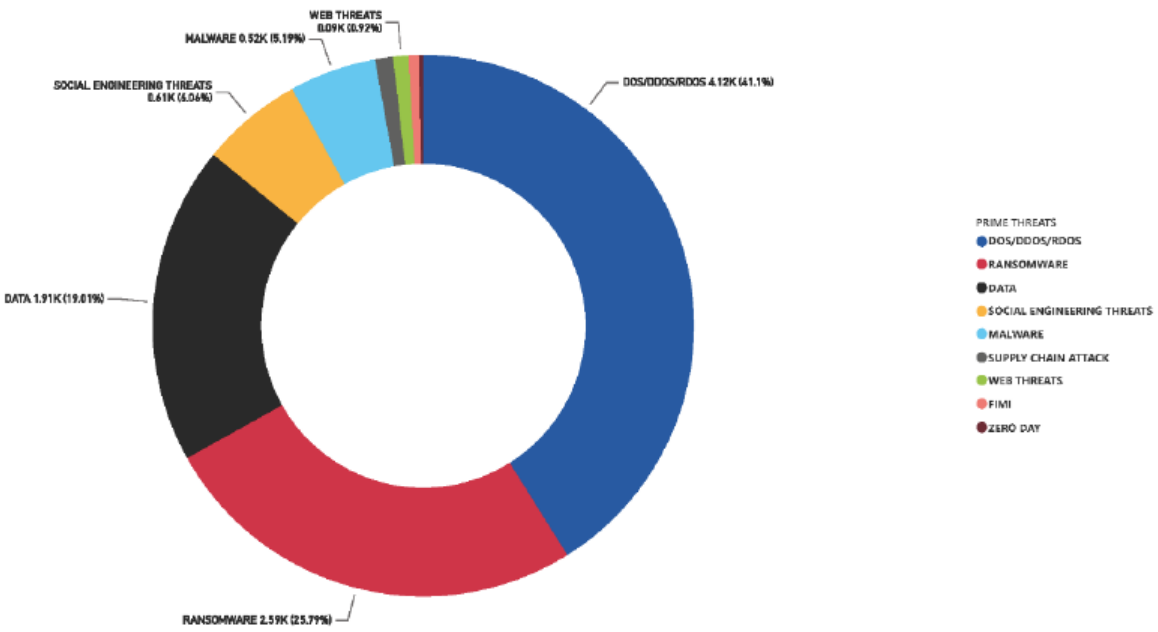
Pohjaksi otettiin Euroopan unionin kyberturvallisuusviraston (European Union Agency for Cybersecurity [ENISA], 2024a) raportti ”*ENISA Threat Landscape 2024*”, koska sen takana ei ole yritysorganisaatioiden mahdollista painolastia myydä omia tuotteitaan painottamalla joitain turvallisuuden osa-alueita toisia enemmän. ENISAn raporttiin verrattiin tämän jälkeen kahden kansainvälisen toimijan (Crowdstrike ja Microsoft) raportteja.

ENISAn raportin mukaan merkittävimpiä kyberuhkia 2023–2024 ovat olleet:

- Tiedon saatavuuteen kohdistuvat hyökkäykset: palvelunestohyökkäykset (DoS & DDoS). Nämä kohdistuvat kaikkiin sektoreihin, mutta julkiset palvelut olivat useimmin kohteena. (ENISA, 2024a, s. 15).
- Kiristysohjelmahyökkäykset (ransomware) ovat toiseksi suurin uhka, ja nämä kohdistuvat eniten liiketoimintapalveluihin, sekä valmistajiin.

- Dataan kohdistuvat hyökkäykset (tiedon manipulaatio ja häirintä) kohdistuivat eniten organisaatioihin, jotka käsittelivät ihmisten henkilökohtaista dataa (PII).
- Sosiaalinen manipulointi/tietojen kalastelu (social engineering) jossa käytetään enemmän valideja käyttäjäoikeuksia, sekä datan ostamisen yleistyminen tietovarkailta (information stealers) joiden käyttö on lisääntynyt merkittävästi osana hyökkäysketjuja. Tälle oli myös tunnusomaista, että hyökkäykset kohdistuivat eniten yksityisiin ihmisiin, ja tämän jälkeen digitaaliseen infraan sekä julkisiin palveluihin.
- Haittaohjelmat (malware), saatavissa entistä enemmän myös palveluna. Näiden kohteena ovat yksityisten ihmisten lisäksi digitaalinen infra sekä julkiset palvelut.
- Toimitusketjuihin kohdistuvat hyökkäykset (supply chain attacks). Näiden osalta huomioitiin, että ne voivat tapahtua hyvin monia tässä listattuja uhkia hyväksikäyttäen.
- Valtiollisen tason kyberuhkat sisältäen informaatiokampanjat ja valetiedon levittäminen (Foreign Information Manipulation and Interference, FIMI).
- Nollapäivähaavoittuvuudet (zero-day vulnerability).

Alla oleva KUVIO 4 näyttää ENISAn raportissa lueteltujen merkittävimpien uhkien prosentuaalisen jakauman raportoitujen ja analysoitujen hyökkäysten mukaisesti:



KUVIO 4: Analysoitujen hyökkäysten jakauma (ENISA, 2024a, s. 9)

Raportissa nostettiin esiin muutama selkeä trendi liittyen yllä oleviin uhkiin:

- Pilvipalveluihin kohdistetut, tai niiden kautta toteutetut hyökkäykset.

- Käyttäjäoikeuksiin kohdistuvat hyökkäykset (identity attacks), joissa olemassa olevat oikeudet hankkimalla ja niitä hyväksikäyttämällä tunkeudutaan järjestelmiin.
- LOTS (Living Off Trusted Sites) ja LOTL (Living Off The Land) joissa hyökkääjät pystyvät entistä tehokkaammin piiloutumaan järjestelmiin ja normaalin verkkoliikenteen sekaan tulematta huomatuiksi ja liikkumaan lateraalisesti järjestelmissä.
- Tekoälyn työkalujen käytön yleistyminen rikollisten keskuudessa.
- Tuotantoympäristön järjestelmiin (Operational technology, OT) kohdistuvat hyökkäykset nostettiin esiin voimistuvana trendinä liittyen Venäjän toimintaan EU:n alueella.

Ensimmäiseksi vertailukohdaksi otettu kyberturvallisuuteen erikoistunut Crowdstrike (2024) nosti vuoden 2024 uhkatilanneraportissaan trendeinä erityisesti:

- Sosiaalisen manipuloinnin/tietojen kalastelun ja näin tai muilla keinoin haltuun saatujen tunnusten hyväksikäytön (nousu 40 %:sta 75%:iin vuosien 2019-2023 välillä).
- Pilvialustoihin ja -toimintoihin kohdistuvat uhat (nousu 75% vuosien 2021-2023 välillä).
- Toimitusketjuihin kohdistuvat uhkatekijät.
- Hallinnoimattomat laitteet ja alustat (mm. elinkaaren päässä olevat, sekä yhdyskäytävälaitteet & ratkaisut). Liittyy myös tuotantoverkkojen järjestelmiin kohdistuviin uhkiin.
- Generatiivinen tekoäly osana muita hyökkäyksiä. Mm. sosiaalinen manipulointi syvävääreennös -teknologiaa (deepfake) käyttäen.
- Kiristysohjelmahyökkäykset nousevat esiin läpi raportin.
- Vaalivaikuttamisen (Yhdysvaltain 2024 presidentinvaalit).
- Käyttäjäoikeuksiin kohdistuviin, tai niitä hyväksikäyttäviin hyökkäyksiin ja uhkiin viitattiin raportissa toistuvasti.
- Palvelunestohyökkäykset nousivat esiin läpi raportin kohdistuen varsinkin valtiollisiin ja kriittisen infrastruktuurin toimijoihin.
- Haittaohjelmat pitävät asemansa yhtenä yleisimmistä hyökkäysvektoreista.
- Tuotantoympäristön järjestelmiin kohdistuvat hyökkäykset osana valtiollisten toimijoiden ja haktivistien operaatioita.
- Järjestelmiin piiloutuminen passiivisilla metodeilla ja lateraalinen liikkuminen järjestelmissä.

Toisena vertailukohtana käytetty Microsoftin "Digital Defense 2024" -raportti (2024) nosti merkittävimmiksi kyberuhkiksi:

- Valtiollisen tason kyberuhkat ja hybridisodankäynti vaikutuksineen sisältäen myös vaalivaikuttamisen.
- Kiristysohjelmahyökkäykset.

- Petokset (sisältäen tietojen kalastelun (phishing) sekä toiseksi henkilöksi tekeytymiseen keskittyvät huijaukset (mm. syvävääreennös, äänimanipulointi tekoälyn avulla jne.).
- Käyttäjäoikeuksiin kohdistuvat hyökkäykset joissa olemassa olevat oikeudet hankkimalla tunkeudutaan järjestelmiin rikollisessa tarkoituksessa.
- Sosiaalinen manipulointi.
- Hajautetut palvelunestohyökkäykset.
- Tuotantoympäristön järjestelmien haavoittuvuudet nostetaan yhä enemmän IT-haavoittuvuuksien rinnalle merkittävänä hyökkäysvektorina.

Sekä ENISA, Crowdstrike että Microsoft huomioivat raporteissaan tekoälyn nousevan merkityksen varsinkin haitallisten verkkohyökkäysten kehittämisessä ja toteuttamisessa, sekä sosiaalisen manipuloinnin, tietojenkalastelun ja informaatiokampanjoinnin tehostamisessa (Crowdstrike, 2024, s. 32; ENISA, 2024a; Microsoft, 2024. s. 83-93). Myös toimittajaketju-uhkat voivat toteutua hyvin monien hyökkäysvektoreiden kautta (ENISA, 2024a, s. 12). Tämä on asia, joista organisaatioiden tulisi tiedostaa toiminnassaan.

Yhteistä ja merkittävää eri uhkille kaikkien raporttien mukaan oli kuitenkin muun muassa se, että hyvin usein niissä hyödynnetään haavoittuvuuksia (esim. järjestelmähaavoittuvuudet, joista ei tiedetä sekä nollapäivähaavoittuvuudet, ja puuttuvat päivitykset), tai käytetään hyväksi inhimillistä tekijää (esim. tietojen kalastelu, sosiaalinen manipulointi, tietovuodot ja petokset, virheet). Esimerkiksi tuotantoympäristöjen järjestelmien osalta Microsoftin raportissa väärät konfiguraatiot olivat päivittämättömien järjestelmien ohella suurin yksittäinen haavoittuvuustekijä (Microsoft, 2024, s. 71-72).

ENISA korostaa raportissaan ”*Foresight Cybersecurity Threats for 2030 update report*”, että riippumatta siitä miten paljon teknologia kehittyy, tai osittain sen vuoksi ihminen toimijana on aina uhka, ja monimutkaistuvalla kentällä osaamiseen ja sitä kautta inhimillisiin virheisiin liittyvät uhkatekijät korostuvat (2024b, s. 10, 12). Tätä on tutkittu monien toimijoiden puolelta, mutta yhtenevästi arviot ihmisestä tietoturvapoikkeamien aiheuttajana ovat 90 % molemmin puolin. Mm. Security Today -verkkoartikkelissa yhteistutkimus Stanfordin yliopiston ja Tessian -turvallisuusyrityksen kanssa johti 88 %:n tulokseen, ja IBM:n toteuttama tutkimus jopa 95 % tulokseen (Ackerman, 2023). Tältä kannalta ihmistekijä on, ja tulee olemaan suurimpia uhkia liiketoiminnan turvallisuudelle ja jatkuvuudelle on kyse sitten osaamisesta, välinpitämättömyydestä, tai tahallisesta toiminnasta.

3.3 Kyberturvallisuuden hallinta organisaatioissa

Tämän kappaleen tarkoituksena on avata asioita, jotka organisaation tulisi huomioida kyberturvallisuutta suunnitellessaan ja ylläpitäessään. Kappaleessa tutkittiin tekijöitä, joiden kirjallisuuskatsauksen perusteella voitiin todeta erottavan

organisaatioita, sekä tukevan eri organisaatioiden kyberturvallisuuden keinoja ja kyvykkyyttä suojata toimintaansa ja sen jatkuvuutta. Tällaisiksi tekijöiksi nousivat johdon tuki, erilaiset lait ja regulaatio, standardit ja viitekehykset, riskienhallinta, turvallisuuskulttuuri ja osaaminen (ihmistekijät), sekä tekniset keinot ja prosessit. Viimeisenä otettiin käsittelyyn edellisessä kappaleessa tehdyt löydökset tämän hetken merkittävimmistä uhkista, ja perehdyttiin niiltä suojautumisen keinoihin.

3.3.1 Turvallisuuden rakentaminen

Yleisellä tasolla organisaation tulee ensin tunnistaa nykytilanne, jossa ollaan. Tämä vaatii aina riskien arviointia, sekä näiden kautta suojattavien kohteiden sekä niihin kohdistuvien uhkien tunnistamista ja tärkeimpien kohteiden priorisoimista. Tähän viittaavat monien muiden ohella mm. Kansainvälinen keskuskauppakamari sekä Kyberturvallisuuskeskus yrityksille ja organisaatioille kohdistetuissa julkaisuissaan (ICC 2016, s. 5; Kyberturvallisuuskeskus 2020, 10-20; Kyberturvallisuuskeskus 2023a; Kyberturvallisuuskeskus 2023b).

Johdon tulee sitoutua selkeästi kyberturvallisuuden rakentamiseen. Lisäksi on kartoitettava minkälaiset uhat organisaatioon kohdistuvat, oltava tietoisia siitä, mikä on merkityksellistä, eli mitä pitää suojata, sekä analysoitava näihin liittyvät riskit tulee varmistaa, että organisaatiolla on olemassa kyberturvallisuusstrategia, tavoitteet, sekä johdon tulee varmistaa lakien, regulaation, mahdollisten standardien, sekä parhaiden tietoturvakäytäntöjen noudattaminen suojattavan omaisuuden turvaamiseksi ennen kuin siirrytään tarkastelemaan havaitsemis-, varautumis-, ja suojautumistoimenpiteitä (ICC, 2016, s.5; Kyberturvallisuuskeskus, 2023a).

Suojautuminen vaatii, että tieto on aina ajantasaista. Tämä tarkoittaa, että on ymmärrettävä mitkä uhat ovat ajankohtaisia. Näitä kartoitettiin edellisessä kappaleessa. Uhkakentän ja riskien ymmärtäminen vaatii jatkuvan tilannekuvan ylläpitoa. Se, mistä tietoa haetaan, riippuu organisaation omasta toimialasta. Käsiteltäessä tutkimuksen rajauksen mukaisesti kyberturvallisuuteen ja jatkuvuuteen liittyvää kenttää voidaan nostaa esiin mm. CVE joka ylläpitää maailmanlaajuista tietokantaa tunnistetuista haavoittuvuuksista (CVE, 2024). Tämän lisäksi esimerkiksi Kyberturvallisuuskeskus tarjoaa Suomessa ajantasaista tietoa kyberuhkista mm. "*Ajankohtaista*" -sivuillaan (Kyberturvallisuuskeskus, 2024). Ajantasaisella tiedolla tarkoitetaan myös teknologian jatkuvan kehityksen uhkien ja mahdollisuuksien ymmärtämistä, sekä tehokkaiden työkalujen käyttöä.

3.3.2 Johdon tuki ja vastuu

Kyberturvallisuudessakin toiminnan ja tuen pitää lähteä ylhäältä alas. Organisaation johdon tulee ymmärtää mitä tulee tehdä suojatakseen organisaatio ja sen ja toiminnot, sekä varmistaa, että näille on jatkuva riittävä resursointi (henkilöt, budjetointi jne.). Johdon sitoutuminen mahdollistaa kyberturvallisuuden toteuttamisen. Lainsäädäntö asettaa johdolle vastuita kyberturvallisuudesta

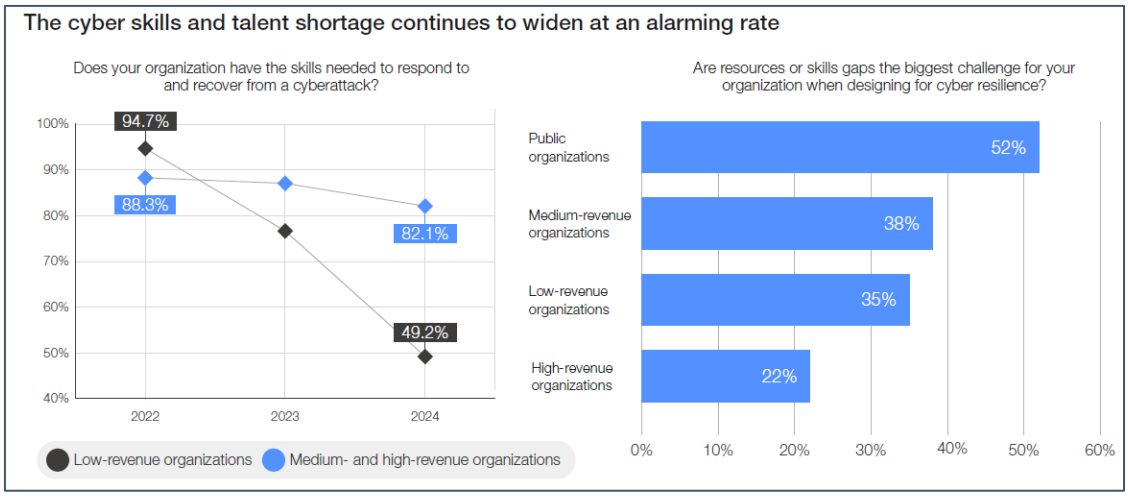
huolehtimiseen. Mm. Euroopan unionin kyberturvallisuusdirektiivi NIS2 (Direktiivi 2022/2555) ottaa suoraan kantaa johdon vastuuseen sen piirissä olevien vaatimusten noudattamisesta kriittiseen infrastruktuuriin kuuluvissa, tai riittävän suurissa organisaatioissa, sekä vaatii myös johdolta tietoturvaosaamista (Loihde, 2024). World Economic Forum (WEF) raportissaan (2024, s. 5-7); 93 % organisaatioista, jotka katsovat olevansa hyvällä tasolla luottavat johdon pystyvän kommunikoimaan kyberriskeistä. Organisaatioissa, joissa kyvykkyyttä ei ole vain 23% uskoo tähän.

Kyberturvallisuuskeskuksen ohjeistukset kyberturvallisuuden vahvistamisesta suomalaisissa organisaatioissa ottavat kantaa mm. juuri liiketoimintakriittisen ympäristön määrittämiseen ja suojaamiseen painottaen johdon vastuuta kokonaiskuvan ymmärtämisessä, muutostarpeissa, resurssien varaamisessa ja kokonaisvaltaisessa valmistautumisessa sekä suojaamisessa asiantuntijoiden ja kumppanien avulla (Kyberturvallisuuskeskus, 2023a).

3.3.3 Erot organisaatioiden valmiuksissa

Yleisellä tasolla vuoden 2024 kyberturvallisuuden tilaa käsittelevässä raportissaan WEF huomioi kasvavat eroavaisuudet organisaatioiden kybertoimintavalmiuksissa, sekä tekoälyn kasvavan merkityksen. Osa organisaatioista on hyvinkin sietokykyisiä kyberuhkille, kun taas toisten valmiudet ovat huomattavasti alhaisemmat. Pääsääntöisesti mitä pienempi organisaatio, sitä heikommat valmiudet. Samoin erot eri toiminta-aloilla vaihtelevat huomattavasti. Siinä missä kyberturvallisuuteen, kriittiseen infrastruktuuriin ja vakuutustoimintaan tai omaisuudenhallintaan keskittyneet toimialat katsovat täyttävänsä vähimmäisvaatimukset kybersietokykynsä puolesta (81–94 %), niin muilla toimialoilla luvut vaihtelevat 38 % ja 81 % välillä (WEF, 2024, s. 14).

WEF nosti raportissaan esiin myös merkittävät erot organisaatioiden välisessä osaamisessa, kyvykkyydessä, sekä resursseissa. Isojen, korkean liikevaihdon omaavien toimijoiden kyvykkyydet ovat parantuneet ja taso on pääsääntöisesti hyvä, kun taas ero pieniin ja varsinkin julkisiin organisaatioihin on resurssien ja kyvykkyyksien puolesta merkittävä (WEF 2024, s. 7-11, 14, 18-19). WEF kuvaa tätä raportissaan (KUVIO 5) josta näkee, että vuosien 2022-2024 välillä alhaisen liikevaihdon organisaatioissa luotto riittäviin taitoihin on pudonnut 45,5% (94,7% →49,2%). Keski- ja korkean liikevaihdon organisaatioissa pudotus oli vain 6,2% (88,3% → 82,1%). Samoin näiden arvioidessa heiltä löytyvää osaamista kyberturvallisuuden suunnitteluun vain 22% suurista organisaatioista koki sen suummaksi haasteekseen, kun taas 52% julkisista toimijoista näki tämän suurimpana haastena. Tässä arviossa pienet (35%) ja keskisuuret organisaatiot (38%) olivat melko lähellä toisiaan.



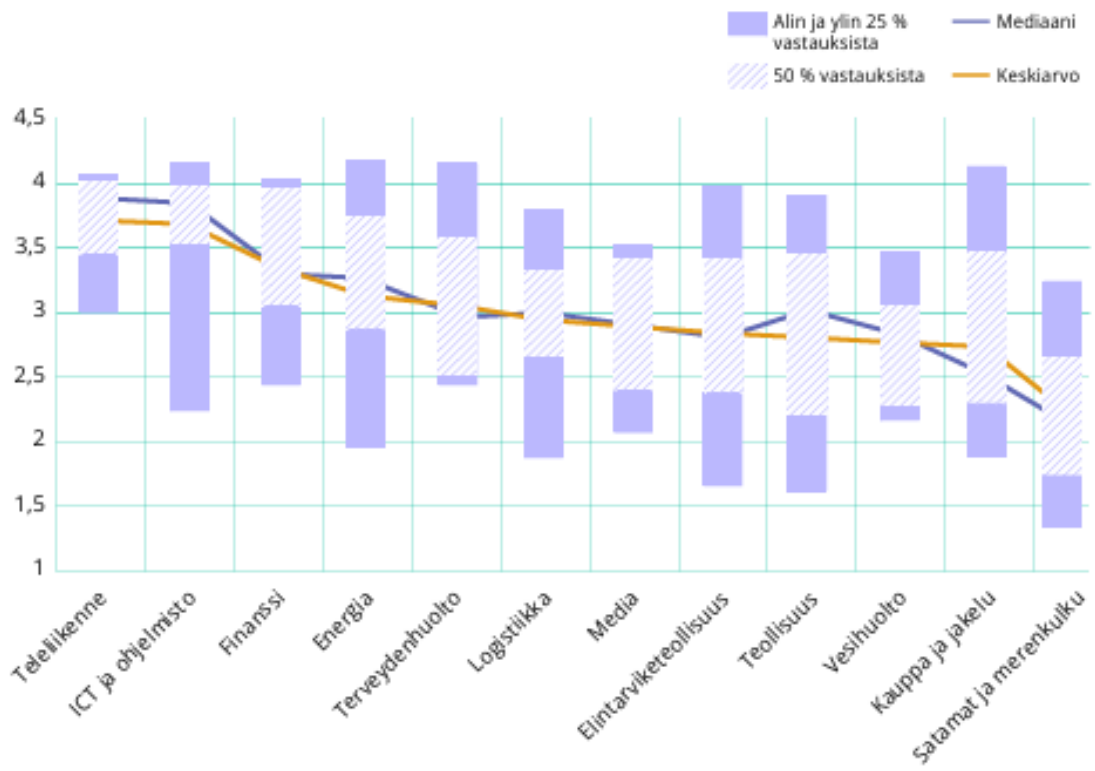
KUVIO 5: Organisaatioiden väliset erot kyberturvallisuuteen liittyvissä taidoissa (WEF, 2024, s. 7)

Ihmisten merkitys organisaatioiden turvallisuudessa on suurempi kuin mikään muu, jota käsiteltiin organisaatioihin kohdistuvia kyberuhkia käsittelevässä edellisessä kappaleessa. Myös lait, regulaatio ja standardit painottavat turvallisuuskulttuurin ja osaamisen merkitystä kyberturvallisuudessa.

Ihmisten kautta tapahtuvilta, tai näiden toiminnasta aiheutuvilta hyökkäyksiltä suojautumiseen tärkeimpinä ovat mm. henkilöstön jatkuvat ja säännölliset tietoturva- ja kyberturvakoulutukset, työ- ja hlökohtaisten laitteiden erottelu, kaksivaiheinen tunnistautuminen, taustaselvitykset, käyttöoikeuksien hallinta (vähimpien oikeuksien periaate), tehtävien eriyttäminen ja riskienhallintaprosessit (ICC 2023; Kyberturvallisuuskeskus, 2020, 26-40; Kyberturvallisuuskeskus 2023a).

Huoltovarmuuskeskuksen ”*Toimialojen kyberkypsyyden selvitys*” -raportissa (2022) kartoitettiin laaja-alaisesti jo toista kertaa huoltovarmuuskriittisten organisaatioiden kyberturvallisuuden tilannetta, kyvykkyyttä ja varautumista toimintaansa kohdistuviin kyberuhkiin, sekä kyberturvallisuuden kokonaishallintaa (HVK, 2022).

Näillä toimialoilla keskiarvollinen tilanne oli hyvällä perustasolla (=keskiarvo 3), mutta eroavaisuuksia toimialojen välillä ja sisällä saattoi olla huomattavasti. Nämä tulevat hyvin selville raportin hajontavertailukuvassa, jossa luetellaan myös tutkimuksen kohteena olleet toimialat (KUVIO 6).



KUVIO 6: Kyberkypsyyden taso ja hajonta organisaatioiden sisällä ja välillä (HVK, 2022, s. 7)

Näiden perusteella voidaan nähdä, että vaikka huoltovarmuuden piirissä olevien organisaatioiden keskiarvoinen suoriutuminen ja varautuminen on melko hyvällä tasolla, niin hajontaa on huomattavasti. Pääsääntöisesti reguloidummat alat kuten Teleliikenne, ICT & Ohjelmisto ja Finanssiala olivat korkeammalla kypsyystasolla (HVK, 2022, s. 14) näiden sisältäessä myös viitekehysten ja standardien käytön. Tämän lisäksi kypsyyttä nostaviksi tekijöiksi katsottiin liiketoiminta- ja riskilähtöinen kyberturvallisuuden kehittäminen ja kommunikaatio johdon ja kyberturvallisuusvastaavien välillä. Vastaavasti laskeviksi tekijöiksi nähtiin Strategisen suunnittelun puutteet, reaktiivisuus uhkiin ja riskeihin, sekä riskienhallinnan käytäntöjen puute (HVK, 2022, s. 11). Suosituksista varautumista edistäviksi tekijöiksi raportissa nostettiin kansallisen varautumisen ulkopuolella: Kyberturvallisuuden strateginen suunnittelu ja hallinnan ja kehittäminen sekä johdon sitouttaminen, kyberriskien käsittely osana kokonaisriskienhallintaa ja uhkien proaktiivinen tunnistaminen, tuotantoympäristöjen turvallisuuden kehittäminen ja toimintojen yhtenäistäminen, sekä tietoturvavalvonnan integroiminen muuhun toimintaan, sekä sovellusturvallisuuden kehittäminen (HVK, 2022, s.9-13).

3.3.4 Tekniset keinot ja prosessit

Teknisten keinojen ja prosessien kirjo on laaja, ja on huomioitava, että aiheen laajuus huomioiden vertailuihin ei voida mennä syvällisemmin, vaan ainoastaan kerätä tärkeimpiä huomioitavia asioita organisaatioita varten.

Esimerkiksi kyberturvallisuusdirektiivi NIS2 (Direktiivi 2022/2555) antaa ohjeita kuinka vaatimukset voidaan toteuttaa, ja Euroopan komissio linjaa toimenpiteitä toimeenpano-ohjeistuksessaan C(2024) 7151 liitteineen (Euroopan komissio C(2024) 7151). Vaikka NIS2 on tarkoitettu kriittiseen infrastruktuuriin kuuluville ja merkittäville toimijoille voidaan sen linjauksia käyttää vertailussa parhaimmista käytännöistä, vaikka organisaatio ei suoraan olisikaan lain vaatimusten alainen.

Tätä kautta kirjallisuuskatsauksessa päätettiin selvittää miten NIS2 vertautuu SFS-EN ISO/IEC 27001:2023 -versioon (2023) joka on laajasti käytössä organisaatioilla. Uutta ISO 27001 -standardia, sekä NIS2 -vaatimuksia on vertailtu useiden toimijoiden puolesta. Näistä valittiin standardeihin ja auditointeihin erikoistuneen BSI Group -yrityksen tekemä kartoitus (BSI, 2024) jonka avulla voitiin tutkia toimenpiteitä, jotka organisaatioiden tulisi huomioida kyberturvallisuutta rakentaessaan:

- Kyberturvallisuuden hallinta (politiikat, lait, auditoinnit, vaatimuksenmukaisuus, koulutukset, henkilötietojen suojaaminen).

Ylempi kohta liittyy NIS2 hallinnollisen johtamisen osuuteen. Seuraavat kohdat liittyvät kyberturvallisuusriskien hallintaan organisaatioissa.

- Tietoturvapolitiikat (kattavat riskianalyysit, järjestelmät ja tiedonhallinnan kyberturvallisuuden, sekä tietoturvariskien hallinta).
- Poikkeamahallinta (tunnistaminen, seuranta, prosessit ja toimintasuunnitelmat tietoturvapoikkeamien varalle, todisteiden keräys, poikkeamista oppiminen).
- Jatkuvuudenhallinta (varmuuskopiointi, toipumissuunnittelu, kriisinhallinta, lokitus, seuranta, poikkeamien aikainen tietoturvahallinta, ICT -jatkuvuudenhallinta).
- Toimitusketjuturvallisuus (tieto- ja kyberturva-aspekti, tietoturvan hallinta toimitusketjuissa, muutoshallinta, pilviturvallisuus, ICT-tietoturvahallinta).
- Verkkoturvallisuus ja verkkopalveluiden turvallisuus (hankinta, kehitys, ylläpito, haavoittuvuushallinta, asian huomioiminen toimittajasopimuksissa, tietoturvapoikkeamahallinnan prosessikuvaukset ja ohjeistukset, tietoturvapoikkeamien raportointi ja käsittely, konfiguraatiohallinta, teknisten poikkeamien hallinta).
- Tieto- ja kyberturvallisuuden hallintamallin ja riskienhallinnan toimivuuden seuranta (seuranta, mittaus, analysointi, arviointi, auditoinnit, johdon vastuu ja ymmärrys tilanteesta).

- Kyberhygienia (mm. pääsynhallinta ja rajoittaminen, poikkeamahallinnan elinkaari, henkilöstömuutosten toimenpiteet, koulutus ja tietoisuus, tunnistaminen, haittaohjelmilta ja viruksilta suojaaminen, varmuuskopiointi, lokitus, verkkojen eriyttäminen, asennuskäytännöt, konfiguraatiohallinta).
- Kryptografia (hallinta, toimenpiteet, ratkaisut).
- Henkilöturvallisuuden tietoturva, pääsynhallinta, sekä liiketoiminta-omaisuuden hallinta (suojattavan omaisuuden tunnistus ja listaus, aineellisen ja aineettoman omaisuuden hallinnan elinkaari, pääsynhallinta, työsuhteen tietoturvan elinkaari sisältäen mm. taustatarkastukset, vaitiolositoumukset, työsuhteen muutokset, huomautukset, sekä työsuhteen loppumisen).
- Monivaiheinen tunnistaminen (tiedonsiirto, pääsyn- ja identiteettihallinta, sekä todennukset).

Viimeiset vertaillut osuudet sisältävät raportointiin ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöä hankkiessaan tuotteita, palveluita tai prosesseja osana kyberturvallisuuden hallintaa.

- Raportointivelvollisuudet (Tiedonsiirto, poikkeamista ilmoittaminen).
- Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttö (tai kyber- ja tietoturvallisuusvaatimusten huomioiminen osana toimittajasopimuksia).

Tämän lisäksi vertailuun otettiin myös Kyberturvallisuuskeskuksen yrityksille suunnatussa ohjeistuksessa (2023a), sekä ICC:n yritysten tietoturvaoppaassa (2016) listattuja suosituksia organisaatioille:

- uhkakuvakentän ajantasaisuus,
- koulutukseen ja informoimiseen panostaminen (turvallisuuskulttuuri ja osaaminen),
- liiketoimintakriittisten ympäristöjen tunnistaminen ja suojaaminen,
- ajantasaiset ja viiveettömät päivitykset (=ajantasaiset järjestelmät),
- automatisoitu varmuuskopiointi ja palautusprosessin varmistaminen,
- virusskannaus,
- turvalliset tietoliikenneyhteydet sisältäen etäyhteydet,
- pilvipalveluiden suojaaminen,
- verkkojen erottelu,
- monikerroksinen suojaaminen / monikerroksiset tietoturvaratkaisut,
- harjoittelu ja testaaminen,
- palomuurit,
- käyttöoikeushallinta,
- haavoittuvuusskannaukset,
- kryptografia,
- vahva salasanavaatimus,
- monivaiheinen tunnistautuminen,

- virus- ja vakoiluntorjuntaohjelmistot,
- sivustorajoitukset,
- järjestelmien ”ylimitoitus” palvelunestohyökkäyksiä vastaan,
- kuormantasaajat, suodattimet, sekä tietoturvapalvelut/-järjestelmät,
- tietoturvaloukkauksiin varautuminen – valmius vastatoimiin,
- toiminnan jatkuvuuden varmistaminen.

Lista on yksityiskohtaisemmin toimenpiteisiin menevä, kuten kuuluukin, koska molemmat toimijat pyrkivät antamaan selkeitä toimenpiteitä kyberturvallisuuden takaamiseksi. Silti listasta voidaan nähdä yhtenevästi samojen asioiden toistumista kuin NIS2 – ISO 27001 -vertailussa.

Suojaustoimenpiteet riippuvat aina suojattavasta omaisuudesta, mutta jokaisella organisaatiolla tulisi olla kyky ensisijaisesti estää, mutta viimeistään havaita poikkeamat mahdollisimman nopeasti ja reagoida niihin riittävän nopeasti merkittävien häiriöiden ja menetysten välttämiseksi. On merkittävää ymmärtää tarpeet nopeaan reagointiin ja vastatoimien aloittamiseen kyberuhkien osalta tapauksissa, joissa hyökkäystä ei ole kyetty estämään. Pahimmillaan vasteaikatarve voi olla vain minuutteja ennen kuin hyökkääjä pääsee toteuttamaan tavoitteensa, tai hyökkäys ehtii aiheuttaa vakavaa vahinkoa (Crowdstrike, 2024, 11-12). Tämä tarve on suuressa kontrastissa siihen mikä keskimäärin on organisaatioiden havainto- ja ilmoitusaika mm. tietomurtoihin liittyen. Esimerkiksi IBM:n vuosittaisessa ”*Cost of Data breach*” -raportissa on vuosien 2017-2023 välillä todettu organisaatioiden havaitsevan hyökkäykset keskimäärin n. 257-280 päivän sisällä hyökkäyksestä. Aikana, jolloin reagointiaika tulisi laskea minuuteissa luku on hälyttävä. Tämän lisäksi vain n. joka kolmas organisaatio havaitsee hyökkäyksen itse (IBM, 2023, s. 6, 14). Yllä olevien tietojen valossa organisaatioilla tulisi olla aina käytössään keinot ensisijaisesti estää hyökkäykset, mutta myös valvoa ja reagoida näihin (ICC, 2016, s. 13). Huomioiden vasteaikavaatimuksen valvonnan olisi suositeltavaa olla 24/7/365 varsinkin, kun vahingot ovat usein rahallisesti merkittävät.

Elinkaariajattelun tulisi olla aina kyberturvallisuuden osana, eikä keskittyä ainoastaan olemassa olevien järjestelmien, laitteiden tai ohjelmistojen turvallisuudesta huolehtimiseen. Organisaatioiden pitää varmistaa, että niiden hankkimat laitteet, ohjelmistot jne. ovat luotettavia ja ylläpidettäviä, sekä huolehtia toiminnassaan alkaen suunnittelun turvallisuudesta esimerkiksi valittavan ”Security by Design” -viitekehyksen avulla, joka ohjaa kaikkea suunnittelua alusta alkaen turvallisuus huomioiden (Microsoft, 2024, s. 10). Esimerkkejä viitekehyksistä ovat mm. NIST SP 800-160 (National Institute of Standards and Technology [NIST], 2021), tai AWS Security by Design (Amazon Web Services [AWS], 2015). Tämän lisäksi mm. DVV on julkaissut turvallisen sovelluskehityksen oppaan (2023b) ja Open Web Application Security Project (OWASP) on järjestö, joka on keskittynyt luotettavan sovelluskehittämisen varmistamiseen ja niiden ylläpitoon (OWASP, 2023). Elinkaariajattelussa suunnittelun jälkeen tulee itse ohjelmointi, testaus, käyttöönotto, ylläpito ja käytöstä poisto. Tulee huomioida, että eri tuotantoympäristöt pitää erottaa myös elinkaariajattelussa, eli testaus- ja

tuotantoympäristöt eivät saisi mennä sekaisin, eivätkä käytöstä poistetut jäädä myöskään pyörimään tuotantoympäristöön miltään osin. (Crowdstrike, 2024, s. 24-25).

Kyberturvallisuudessa eräänä perusperiaatteena toimii mm. nollaluottamusmalli (zero-trust) jonka ajatuksena on, että mihinkään verkossa ei tule luottaa, vaan kaikki tulee varmistaa, käyttöoikeudet minimoidaan ja hyökkäyksiä oletetaan tapahtuvan, eikä ajatusmallia rajata vain ulkoisiin toimijoihin vaan myös sisäisiin (Microsoft, 2023, s. 3-6). Tätä käytetään enemmän verkkoarkkitehtuurissa, mutta ajatusmallia voi hyödyntää myös riskiarvioinneissa muussakin toiminnassa.

Ylläolevien toimenpiteiden keräys ei ole kattava, vaan siinä pyrittiin tunnistamaan ja valitsemaan tutkitun materiaalin avulla toistuvia keinoja. Tässä tutkimuksessa ei pystytä linjaamaan kaikkia toimenpiteitä joita organisaatioiden tulisi huomioida toiminnassaan.

3.3.5 Toimitusketjut

Toimitusketjut on nostettu yhdeksi merkittävimmistä uhkista organisaatioiden liiketoiminnalle ja jatkuvuudelle jo edellä useiden tutkimusmateriaalien pohjalta. Näiden aiheuttamien uhkien ja riskien ymmärtäminen, sekä riippuvuussuhteiden kartoittaminen on ensisijaisen tärkeää, sillä ketjut ovat nykyisin erottamaton osa kaikkea liiketoimintaa. Tämä koskee niin tuotteita, palveluja, järjestelmiä, ohjelmistoja, logistiikkaa, kuin lähes mitä tahansa suojattavaa omaisuutta. Organisaation tulee miettiä mihin asti toimitusketjujen turvallisuus tulee, ja on kannattavaa varmistaa. Vaatimuksia ja linjauksia tähän tuovat lait, direktiivit ja standardit (mm. direktiivi NIS2 2022/2555; SFS-EN ISO/IEC 27001:2023, 2023) sekä kyberpolitiikan, vaatimusten valvontaan, kehittämiseen ja ohjaukseen keskittynyt ENISA (Direktiivi 2019/881).

3.4 Yhteenveto

Kyberturvallisuuden rakentaminen on pitkäaikainen ja monimutkainen prosessi, ja kaikkien uhkien ja riskien tunnistaminen on haastavaa. Johdolla on hyvin iso, niin lainmukainen kuin liiketoimintaan liittyvä vastuu mm. organisaatioiden kyberturvallisuuden toteutumisesta, ja heidän tuellaan tulee varmistaa riittävät toimenpiteet ja osaaminen.

Ensisijaisesti kyberturvallisuuden pitäisi olla aina ehkäisevää, ennakoivaa ja proaktiivista. Kuitenkin hyökkäyksen / tietoturvaloukkauksen sattuessa on tärkeää huomioida miten nopeasti tapahtuma voi edetä, ja kuinka nopeasti näihin pitää pystyä organisaatioiden puolelta reagoimaan, analysoimaan tapahtumat sekä estämään / rajoittamaan vahinkoja ja huolehtimaan palautustoimista.

Lait ja standardit asettavat vaatimuksia, sekä antavat raameja kyberturvallisuuden tehokkaampaan toteuttamiseen. Vaikka organisaatio ei päättäisi

hankkia sertifikaattia joltain osa-alueelta on sen suositeltavaa tutustua ns. parhaisiin käytäntöihin, joita standardeissa on tunnistettu, jotta se voi paremmin valita omat suojaustoimenpiteensä.

Huomioitavaa on myös, että organisaatioiden kyvykkyydet vaihtelevat huomattavasti koosta ja liikevaihdosta riippuen. Silti jokaisen organisaation tulisi tunnistaa ja priorisoida omaa toimintaansa koskevat tärkeimmät suojattavat kohteet ja miettiä näille riittävät suojaustoimenpiteet, sekä kouluttaa henkilöstönsä ymmärtämään tieto ja kyberturvallisuuden vaatimuksia ja organisaatioon kohdistuvia uhkia. Henkilöstön kouluttaminen on kustannustehokas tapa varmistaa turvallisuutta huomioiden ihmistekijän suuri prosentuaalinen osuus tietomurroissa ja tietosuojaloukkauksissa.

Kyberturvallisuudesta huolehtiminen on jatkuvaa työtä, ja silti on olemassa suuri riski sille, että uhkaa tai riskiä ei tunnisteta, hallinta on joltain osin vajavaista, tai toimenpiteet ovat liian hitaita. Organisaation tulee aina varautua myös siihen pahimpaan, että tapahtuu jotain, joka vaarantaa organisaation toimintaedellytykset ja tulevaisuuden, ja suunnitella toimenpiteet näihin varautumiseen.

4 YHTEISET TEKIJÄT

Tässä luvussa käsitellään sekä jatkuvuudenhallintaa että kyberturvallisuutta yhteisesti koskevia osa-alueita, jotka ovat tulleet ilmi kirjallisuuskatsauksessa, eikä niitä nähty järkeväksi kirjoittaa molempiin erikseen. Suojattavan omaisuuden ja toimintojen tunnistaminen, johdon rooli, vastuut ja resursointi käsiteltiin kuitenkin jo jatkuvuudenhallintaa koskien tämän tutkimuksen kappaleessa 2.2, sekä kyberturvallisuuden osalta kappaleissa 3.3 ja 3.4 joten niitä ei käsitellä uudestaan tässä luvussa.

4.1 Ohjaava regulaatio

Monet lait ja standardit, jotka liittyvät tietoturvallisuuteen yhdistävät jatkuvuudenhallinnan ja kyberturvallisuuden osaksi vaatimuksia. Kappaleessa käydään läpi tämänhetkistä yleisintä lainsäädäntöä, regulaatiota, viitekehyksiä, standardeja sekä kriteeristöjä läpi. Lista ei pyri olemaan kattava aiheen laajuuden vuoksi, vaan antamaan tietoa tutkimuksessa yleisimmin vastaan tulleista materiaaleista.

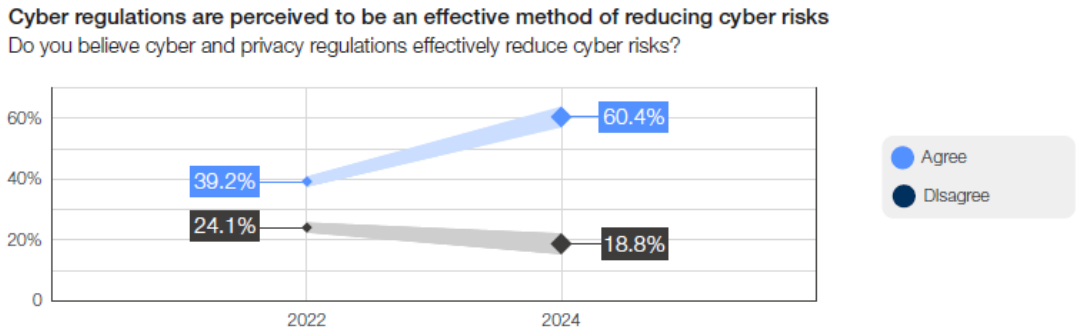
4.1.1 Lait ja määräävä regulaatio

Lakien, määräysten, säädösten ja asetusten, sekä viranomaisten ohjaavan dokumentaation merkitystä ei voida ohittaa puhuttaessa organisaatioiden kyberturvallisuudesta tai jatkuvuudenhallinnasta. EU ja Suomi kehittävät jatkuvasti varsinkin kyberturvallisuuteen liittyvää lainsäädäntöään ja ohjaavaa dokumentaatiotaan (mm. strategiat) vastaamaan nykyisiä sekä kehittyviä uhkia ja vaatimuksia vastaavaksi, ja näissä on huomioitu myös jatkuvuudenhallinta osa-alueenaan tai vaatimuksiin integroituna. Näistä merkittäviä ovat mm. päivitetty kyberturvallisuusdirektiivi NIS2 (Direktiivi 2022/2555) jonka vaatimuksiin sen piirissä olevien organisaatioiden tuli vastata 18.10. 2024 (Eurooppa-neuvosto 2024a). NIS2 -direktiivi ottaa kantaa myös jatkuvuudenhallintaan kyberturvallisuuteen liittyen (2022/2055, 21. artikla). Vaikka laki kohdistuukin keskisuuriin ja suurin organisaatioihin, sekä kriittiseen infrastruktuuriin se sivuaa hyvin monia muitakin suoraan tai välillisesti mm. toimitusketjujen hallinnan kautta. Tämän lisäksi merkittävä on EU:n Kyberturvallisuusasetus joka määrittelee EU :n kyberturvallisuusvirasto ENISA :n toimintaa ja EU :n laajuisten kyberturvallisuuden sertifiointijärjestelmien kehittämistä ja käyttöönottoa (Direktiivi 2019/881). Esineiden internetin haasteisiin vastaamaan on tulossa kyberkestävyyssäädös joka asettaa vaatimuksia digitaalisia elementtejä sisältäville tuotteille. Laki on hyväksytty Eurooppa-neuvostossa ja sitä aletaan soveltaa tulevaisuudessa (Eurooppa-nevosto, 2024b).

Organisaatioiden kyberturvallisuutta säätelevillä laeilla ja regulaatiolla on perustavanlaatuinen rooli kyberuhkiin varautumisessa, sillä toisin kuin monet muut keinot, ne eivät ole ohjaavia, vaan määrääviä

Tällä hetkellä organisaatioita laajemmin koskettavaa kyberturvallisuutta Suomessa ja EU:ssa on tullut voimaan, ja lisää ohjaavaa lainsäädäntöä on tulossa. Nick Kirtley avaa ja vertailee näitä verkkoartikkelissaan (2024). Nykyistä ohjaavaa lainsäädäntöä ovat mm. kriittiseen infraan ja merkittäväksi luokiteltaville yrityksille tarkoitettu aiemmin mainittu jo voimaan tullut kyberturvallisuusdirektiivi NIS2 (Direktiivi 2022/2555). Tulevaa lainsäädäntöä ovat mm. DORA -asetus (Digital Operational Resiliency Act) joka on kohdistettu finanssialan yrityksille ja niiden toimijoille (Euroopan komission asetus 2022/2554) joka tulee voimaan 17.5.2025, Kyberresilienssisäädös (Euroopan komissio, 2023) joka määrittää turvallisuusvaatimuksia sekä laitteistoille että ohjelmistoille tullen voimaan 2027, ja 2026 voimaantuleva Tekoälysäädös (Artificial Intelligence Act) joka linjaa riskiperusteisia vaatimuksia tekoälyn käyttöön (Euroopan komission asetus 2024/1689 ; 2024 Kirtley, 2024). Jatkuvuudenhallintaa koskevaa lainsäädäntöä ja regulaatiota on paljon vähemmän ja se keskittyy kriittisen infrastruktuurin turvaamiseen.

Kaikki nämä ohjaavat kyberturvallisuutta hallitumpaan ja reguloidumpaan suuntaan mikä omalta osaltaan auttaa organisaatioiden valmiuksia vastata uhkiin ja koetaan näiden puolelta tehokkaaksi kyberriskien vähentäjäksi kuten alla olevassa kuvassa (KUVIO 7) nähdään (WEF, 2024, s.7), mutta myös lisää riskejä regulaatiokentän monimutkaistuessa joka voi itsessään johtaa poikkeamiin ja vaikeaan hallittavuuteen (ENISA, 2024a, s. 73; WEF, 2024, s. 31).



KUVIO 7: Kyberturvallisuutta ohjaavan regulaation koettu vaikutus (WEF, 2024)

4.1.2 Viitekehykset, standardit ja kriteeristöt

Viitekehysten tarkoituksena on antaa organisaatioille strukturoitu malli joka ohjeistaa standardimaisiin parhaisiin käytäntöihin turvallisuuden riskienhallinnan tukena (Taherdoost, 2022b).

ISO -standardit tarjoavat viitekehyksen omille standardeilleen, joita tähän tutkimukseen liittyen ovat mm. jatkuvuudenhallinnan standardi (SFS-EN ISO 22301:2019, 2019) ja tietoturvallisuuden hallinnan standardi (SFS-EN ISO/IEC 27001:2023, 2023), sekä sitä tukevat hallintakeinot (SFS-EN ISO/IEC 27002:2022,

2022), joka sisältää ohjeita ISO 27001 viitekehyksen ja hallintamallin toteuttamiseen. Se sisältää sekä jatkuvuudenhallinnan että kyberturvallisuuden hallinnan osaksi kokonaisviitekehystä ja kontrollejaan. Kyberturvallisuutta ohjaavat kontrollit löytyvät varsinkin standardin kappaleesta 8. teknologisten kontrollien alta. Jatkuvuudenhallintaa vaativat kontrollit taas ovat jakautuneet neljän osa-alueen (organisaation valvonta, ihmiset, fyysinen ja teknologinen) välille, mutta uusi standardi ottaa vahvemmin kantaa toiminnan jatkuvuuden varmistamiseen (Edwards, 2022; SFS-EN ISO/IEC 27001:2023, 2023). ISO 22301 taas noudattaa ISO-standardien viitekehystä keskittyen kuitenkin jatkuvuudenhallintaan (SFS-EN ISO 22301:2019, 2019).

Kyberturvallisuudessa käytetään monia viitekehyksiä ohjaamaan toimintaa. Tässä keskityttiin niihin jotka ovat yleisemmin käytössä Suomessa tai EU -alueella, eivätkä ole kohdistettu mihinkään tietyntyyppiseen toimintaan. Organisaation tulee aina valita viitekehyksensä omaan toimintaansa ja tarpeisiinsa sopivaksi, mutta monet antavat yleisrakenteen kyberturvallisuuden hallintaan. Viitekehyksistä käytetyimpiä ovat aiempien tutkimustuloksten perusteella mm. National Institute of Technologyn (NIST) Cyber Security Framework (NIST CSF) ja ISO 27000 -sarjan standardien mallit (Folorunsho, Ayinde, Olagoke, & Fatoye, 2019; Taherdoost, 2022b).

Siinä missä lait, asetukset, sekä viranomaismääräykset ovat ehdottomia vaatimuksia, jos ne koskevat organisaatiota, niin standardien avulla saadut sertifikaatit ovat pääosin vapaaehtoisesti hankittavia todennuksia organisaation vaatimuksenmukaisuudesta ja hyvästä asioiden hoidosta tarkasteltuun osa-alueeseen nähden. Näiden merkitystä ei kuitenkaan tule väheksyä, sillä niiden avulla organisaatio pystyy usein paitsi vastaamaan lainsäädännön vaatimuksiin, myös tunnistamaan parhaita käytäntöjä joiden avulla parantaa turvallisuuttaan. Tieto- ja kyberturvallisuuteen liittyviä standardeja on useita. Yleisimpiä tietoturvallisuutta käsitteleviä standardeja ovat jo aiemmin mainittu ISO 27000 -sarja joka keskittyy kokonaisvaltaisesti tietoturvallisuuden hallintakehykseen. Sarjan standardeja on yhteensä 46 kappaletta, yleisimpänä Euroopassa jälleen ISO 27001 joka on tietoturvallisuuden ohjaavan hallintakehyksen kokonaisvaltainen standardi (ISMS, ei pvm. ; SFS 27001:2023, 2023). Jatkuvuudenhallinnan standardina taas on SFS-EN ISO 22301 :2019 (SFS 22301 :2019, 2019)

Viranomaispuolella merkittävimpiä ovat arviointikriteeristöt jotka keskittyvät Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseen turvallisuuden hallintakehyksillä ja keinoilla & vaatimuksilla. Näistä useimmin käytetty on Kansallisen turvallisuusviranomaisen (NSA) Tietoturvallisuuden auditointityökalu viranomaisille (Katakri 2020) joka keskittyy turvallisuusjohtamiseen (prosessit), fyysiseen turvallisuuteen, sekä tekniseen turvallisuuteen (Kansallinen turvallisuusviranomainen [NSA], 2020). Toinen on Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri (Traficom, 2020) jonka tavoitteena on turvata em. tieto jos sitä säilytetään pilvessä. Kolmas on julkisen hallinnon tietoturvallisuuteen kohdistuva arviointikriteeristö Julkri (VM, 2023) jonka kohteena on julkishallinto ja joka sisältää osia kahdesta

aiemmasta. Vaikka kaikki edellämainitut liittyvät viranomaistoimintaan ja julkishallintoon niillä on arvoa hyvien käytänteiden tarkastelussa myös organisaatioissa, vaikka em. luokiteltua tietoa ei käsiteltäisikään. Tieto- ja kyberturvallisuutta sekä jatkuvuudenhallintaa ohjaavia standardeja, viitekehyksiä ja ohjeistuksia joihin organisaatioiden on hyvä tutustua on edellä mainittujen lisäksi useita, mutta nämä tulee aina valita omien tarpeiden, toimintojen ja mahdollisten asiakasvaatimusten mukaisesti.

4.2 Riskienhallinta

Riskienhallinta on osa-alue jonka katsotaan olevan aina kriittinen osa toimintoja ja organisaation johtamista, ja johon velvoittavat lukuisat lait ja standardit. Mm. NIS2 vaatii kyberturvallisuusriskien hallintaa, ja ISO -standardit jotka ovat varsinkin yritysorganisaatioissa usein vaadittuja vaativat prosessinomaista riskienhallintaa. Näitä ovat jo aiemmin läpikäytyjen ISO 27001- ja ISO 22301 -standardien lisäksi mm. Laadunhallintajärjestelmän standardi ISO 9001 (SFS-EN 9001 :2015, 2015). Aihealue on niin merkittävä, että sille on myös oma riskienhallinnan standardi SFS-ISO 31000 :2018 (2018).

Riippumatta mistä turvallisuuden osa-alueesta puhutaan, niin riskienhallinta nousee aina esiin yhtenä kaiken toiminnan peruspylväistä. Riskienhallinta on prosessi jolla ”*tuetaan organisaatioiden tavoitteiden saavuttamista ja toimintaan liittyvien mahdollisuuksien ja uhkien tunnistamista*” (VM, ei pvm.). Valtiovarainministeriön julkaisussa Kimmo Rousku kuvaa riskienhallinnan merkitystä: ”*Digitaalisen turvallisuuden eli muun muassa tieto- ja kyberturvallisuuden sekä tietosuojan taustalla tärkeimpänä prosessina vaikuttaa oikein toteutettu ja toimiva riskienhallinta*.” (Rousku, 2017). SFS-ISO 31000:2018 (2018) määrittää riskienhallinnan viitekehyksen, jota mukaillen Rousku on tehnyt alla olevan kuvan (KUVIO 8) Valtiovarainministeriön julkaisussa ”Ohje Riskinhallintaan” (Rousku, 2017, s. 12).

KUVIO 8 Riskienhallinnan viitekehys SFS-ISO 31000 mukaillen (Rousku, 2017)

Kuvassa tulee esille riskienhallinnan kokonaisuus, joka sisältää toimintaympäristön määrittelyn, riskinarvioinnin kokonaisprosessin ja riskien käsittelyn, sekä kommunikaation ja seurannan. Näitä ei voida toteuttaa ilman vaadittavia politiikkoja, toimintamalleja ja ohjeistuksia, ja tulee muistaa, että riskienhallinnan tulee kattaa myös ulkoinen toimintaympäristö sidosryhmineen, ei vain sisäisiä. Edellä mainittujen asioiden tulee toteutua turvallisuuden osa-alueesta riippumatta, mutta osittain näitä tulee pystyä yhdistämään mahdollisimman tehokkaan riskienhallinnan varmistamiseksi.

4.3 Yhteistä tutkimusta

Molempia osa-alueita tarkemmin käsitteleviä ohjeistuksia tai tutkimuksia löytyi mm. ”*ICT-varautumisen vaatimukset*” Valtiovarainministeriöltä osana VAHTI -ohjeita jotka ohjaavat hallinnonalojen organisaatioita ja ministeriöitä, mutta joita voidaan käyttää hyvien toimintatapojen ohjeina myös muissa organisaatioissa (VM, 2012). Tämän lisäksi useat, varsinkin kriittiseen infrastruktuuriin liittyvät tutkimukset ottavat kyllä kantaa jatkuvuudenhallintaan (mm. Lehto, 2023; Neittaanmäki ym., 2021; VM, 2016b), mutta osa-alueita laajemmin käsittelevää tutkimusta, joka olisi kohdistettu muihin kuin kriittiseen infrastruktuurin liittyviin toimijoihin ja viranomaisvaatimuksiin liittyen ei tutkimuksessa löytynyt.

Digi- ja Väestötietovirastolta (DVV) löytyi kuitenkin vuosittain digiturvakysely (DVV, 2023a) julkisen hallinnon organisaatioille. DVV:n kysely antaa kuvaa tilanteesta julkishallinnon ja viranomaisten puolella, mutta ei avaa huomattavasti kirjavamman organisaatiokentän tilannetta. Digiturvakyselyn tuloksissa on kuitenkin huomioitu sekä kyberturvallisuus, että toiminnan jatkuvuus ja varautuminen omina osa-alueinaan. Vuoden 2023 kyselyyn on saatu vastauksia 194:ltä julkisen hallinnon organisaatiolta, jotka ovat antaneet arvion osa-alueesta 0-1 välillä. Mitä lähempänä arvoa 1 tulos on sitä paremmin organisaatiot ovat katsoneet suoriutuneensa kyselyn väittämistä. Alla eri osa-alueiden keskiarvot (TAULUKKO 1):

TAULUKKO 1 DVV:n digiturvakyselyn osa-alueiden keskiarvot (DVV, 2023)

	2023	2022	2021
Koko kysely	0,70	0,69	0,71
Johtaminen	0,65	0,65	0,65
Riskienhallinta	0,68	0,70	0,68
Toiminnan jatkuvuus ja varautuminen	0,66	0,67	0,67
Tietoturvallisuus	0,75	0,75	0,78
Tietosuoja	0,78	0,77	0,81
Kyberturvallisuus	0,61	0,59	0,59

Taulukon perusteella voidaan todeta, että muutosta ei ole juurikaan tapahtunut vuosien 2021-2023 välillä. Kyselyn tarjoamaa dataa käytettiin analysointivaiheessa vertailussa muihin löydöksiin.

5 KYBERMAAILMAN UHKIEN KEHITYS TULEVAISUUDESSA

Tutkimus pyrki painottumaan vahvasti paitsi nykytilanteen ymmärtämiseen, myös tulevaisuuden trendien ja uhkien hahmottamiseen, jotta organisaatiot voisivat varautua ennakoivasti tuleviin jatkuvuuteensa vaikuttaviin kyberuhkiin.

Kybertoimintaympäristö kehittyy koko ajan merkittävästi, mutta silti tulee huomioida, että vanhemmat uhat eivät pääasiallisesti poistu, vaan kehittyvät ja muuttavat muotoaan. Materiaaleissa nousi esiin tekijöitä, jotka ovat sekä mahdollisuuksia että uhkia, mutta jotka joka tapauksessa tulevat muuttamaan ja laajentamaan kyberuhkakenttää. Tutkimukseen valittiin aineistoksi kaksi päälähdettä jossa uhkia oli selvitetty laajemmin; ENISA käsittelee vuoden 2023 raportissaan ”*Identifying emerging cyber security threats and challenges for 2030*” arvioituja kyberuhkia kuuden vuoden kuluttua (ENISA, 2023), sekä Valtioneuvoston kanslian (VNK) ”*Suomen Kyberturvallisuusstrategia 2024-2035*” (VNK, 2024). Tämän lisäksi tarkasteluun valittiin joitakin kehittyviä teknologioita, joilla on potentiaalia aiheuttaa tulevaisuudessa merkittäviä uhkia.

ENISAn raportissa (2023, s. 8, 11-20) nostettiin merkittävimmiksi uhkiksi seuraavat alla olevassa järjestyksessä merkittävimmästä alkaen:

1. Ohjelmistojen riippuvuus toimitusketjuista komponentti-integraatioiden vuoksi (ohjelmistot, laitteistot ja komponentteihin keskittyvä koodaus). Tämä heikentää ketjujen näkyvyyttä ja hallittavuutta ja lisää rikollisten toimijoiden hyökkäysmahdollisuuksia.
2. Kehittyneet valeinformaatio- ja vaikuttamiskampanjat tekoälyä (mm. syväväärennökset) hyväksikäyttäen pääasiassa valtiollisten tahojen ja tai poliittisesti motivoituneiden toimijoiden taholta.
3. Digitaalisen valvonnan autoritäärisyyden vahvistuminen / Yksityisyyden menetys, kun teknologiaa käytetään esim. valtiollisten toimijoiden taholta seurannassa ja tunnistamisessa (esim. kamerat julkisilla paikoilla). Tämä voi johtaa haasteisiin ihmisten yksityisyyden osalta, näiden tietovarantojen samalla houkutellessa rikollisia.
4. Inhimilliset virheet ja vanhojen järjestelmien (haavoittuvuuksien) hyödyntäminen kyberfyysisessä ekosysteemissä. Tämä uhka liittyy laajaan esineiden internetin (IoT) hyödyntämiseen ja älylaitteiden määrän kasvuun. Tätä kautta myös huonosti suojattujen ja päivittämättömien laitteiden määrä kasvaa, eikä inhimillisiltä virheiltä ja osaamiseen liittyviltä haasteilta vältytä. Tämä johtaa kasvaviin haasteisiin sekä IT:n että tuotantoympäristöjen järjestelmien osalta.
5. Älylaitteiden hyödyntäminen kohdistetuissa hyökkäyksissä. Tässä uhassa älylaitteiden keräämän datan määrä on kasvanut merkittävästi johtaen myös käyttäjien toiminnan ja tapojen tarkempaan seurantaan, johon voi liittyä myös sensitiivistä tietoa (esim. terveystietoja). Tämä kasvattaa hyökkäyspinta-alaa mm. erilaisten haittaohjelmien kautta.

6. Puutteet avaruuteen sijoittuvan infrastruktuurin ja kohteiden analysoinnissa voivat nopeasti kehittyessään johtaa kilpailun ja nopean kehittämisen tarpeen kautta kriittisiin puutteisiin analysoinnissa.
7. Hybridiuhkien nousu tarkoittaa hienostuneempien kyberhyökkäysten kehittymistä, joihin liittyy myös fyysinen tai muuten ei -verkkoon kohdistuva aspekti. Tällaisilta hyökkäyksiltä puolustautuminen, tai niiden tunnistaminen on vaikeampaa monipuolisemman uhkakentän vuoksi.
8. Osaamispuutteiden arvioidaan olevan vieläkin merkittävimpiä uhkia turvallisuudelle. Tätä ei uskota pystyttävän ratkaisemaan vuoteen 2030 mennessä, päinvastoin nopeasti kehittyvä teknologia eskaloi uhkaa.
9. Rajojen yli ulottuvat tieto- ja viestintäteknologiaan (ICT) liittyvät palvelut yksittäisenä (kriittisenä) vikapisteenä johtuu fyysisen infrastruktuurin riippuvuudesta verkosta. Suurin osa infrasta tarvitsee näitä palveluita toiminnassaan. Tähän liittyvät paitsi maarajat, myös satelliittien toiminta ja älykaupunkien verkottuneisuus tarjoten houkuttelevan kohteen vihamielisille toimijoille.
10. Tekoälyn hyväksikäyttö nousee koko ajan suuremmaksi riskiksi, kun käyttö laajenee, eikä opetusmallien eettisyyttä voida varmistaa, ja riskit tekoälyn väärinoppimiselle tai manipuloinnille (ja näin virheille) kasvavat. Generatiivinen tekoäly tuo omat ulottuvuutensa uhkaan.

Tämän lisäksi ENISA (2023, s. 21-23) arvioi muiksi uhiksi digitaaliseen valuutan lisääntyvän käytön rikollisuudessa, geneettisten & sähköisten terveystietojen hyväksikäytön, syvävääreennös -teknologian kehittymisen ja hyödyntämisen, kvanttiteknologian käytön hyökkäysten toteuttamisessa, erilaisten monimutkaisiin järjestelmäekosysteemeihin liittyvien haavoittuvuuksien hyväksikäytön, lohkoketjuteknologioiden yhteensopimattomuuden ja käyttöhäiriöt, sekä ilmastonmuutoksen vaikutukset kriittiseen ICT -infrastruktuuriin.

Suomen kyberturvallisuusstrategiassa, vaikka asiaa käsitelläänkin enemmän valtiollisen tason näkökulmasta, voitiin silti nostaa esiin seuraavia oletettavia trendejä kyberuhkissa (2024, s. 13-26):

1. Kyberympäristön hyödyntäminen hybridivaikuttamisessa.
2. Laiton tiedonhankinta eri keinoin.
3. Fyysiset uhat kybertoimintaympäristölle (sähkön saannin häiriöt, luontoon liittyvät uhkatekijät, inhimilliset virheet).
4. Vihamielisen kybertoiminnan lisääntyminen (tämä voi tapahtua millä tahansa keinoin).
5. Teknologinen murros sisältäen:
    a. Verkkoon yhteydessä olevien laitteiden määrän kasvu jopa miljardeilla vuoteen 2030 mennessä.
    b. Inhimilliset virheet ohjelmistokehityksessä ja niiden toimitusketjuissa, sekä tarkoitukselliset haavoittuvuudet.
    c. Tekoälyn, kvanttilaskennan, pilvipalveluiden, 6G - ja satelliittiteknologian nopea kehitys.

6. Globaalien toimitusketjujen alttius häiriöille ketjujen pidentyessä ja monimutkaistuessa, sekä yleisesti toimitusketjujen kautta realisoituvat uhat.
7. Kvanttiteknologian uhka salauskyvykkyydelle, kun nykyiset salausratkaisut ja -algoritmit eivät enää riitä.
8. Inhimilliset virheet nousevat esiin useassa kohdassa strategiaa.

Merkittävinä uusina trendeinä, jotka eivät ole vielä täysipainoisesti toteutuneet, mutta tulevat kehittymään voidaan pitää tekoälyn kehitystä joka kattoterminä keskittyy rakentamaan ja hallitsemaan itsenäiseen päätöksentekoon ja oppimiseen kykenevää teknologiaa jonka alle kuitenkin asettuu niin ohjelmistoja kuin laitteistojakin (Rouse, 2024). Kvanttiteknologiaa monissa eri muodoissaan, jonka avulla pystytään käsittelemään ja analysoimaan tehokkaammin mm. massadataa ja tietoaltaita on kehittyvä trendi (Neittaanmäki ym., 2021, s. 77-85). Molemmat ovat sekä uhkia että mahdollisuuksia, mutta joka tapauksessa niitä ei saa jättää huomioimatta kyberturvallisuutta ja jatkuvuudenhallintaa varmistettaessa, ja molempien nopea kehitys tällä hetkellä on huomioitava. Tulevaisuudessa myös tiedonsiirtonopeudet tulevat tukemaan massadatan käsittelyä, sekä tekoälyn ja kvanttiteknologian vaatimuksia, sillä 5G:n seuraajan 6G:n, joka tukee monimutkaisten älyjärjestelmien ja mm. virtuaalitodellisuusratkaisuiden tarpeita on arvioitu tulevan kuluttajien käyttöön n. 2030 (Elo, 2024).

Seuraavissa alaluvuissa nostetaan lyhyesti esiin teknologioita, jotka on voitu tunnistaa jo kyberuhkiksi nyt tai lähitulevaisuudessa, tai sitten niiden kehitys on vielä epäselvää, mutta ne voivat olla merkittäviä uhkavektoreita pidemmällä tähtäimellä.

5.1 Teknologia ja laitteistot

Yllä olevien lisäksi voidaan nostaa esiin teknologiaa, joista osa on vasta kehitysvaiheessa, eikä vielä yleisesti saatavilla, mutta näitä tulee silti seurata, ja miettiä aiheutuvia kyberuhkia. Tällaisia ovat mm. Laitteiden jatkuva pieneminen ja tehokkuuden / tarkkuuden parantuminen (mm. kamerat, tietokoneet). ”Teratavumaailmassa” älypuhelimet voivat käsitellä suuria määriä dataa (Neittaanmäki ym., 2021, s. 50). Pienin kehitetty tietokone, laite 0,3 mm kokoinen (June, 2015) on jo nanoteknologiaa, joka myös on koko ajan kehittyvä tieteenala. Vaikka toistaiseksi nanoteknologiasta puhutaan tieteellisiä artikkeleita tarkasteltaessa lähinnä lääketieteen, sota- ja puolustusteollisuuden, sekä avaruusteknologian kannalta, niin huomio on myös jo IoT:n ja nanoteknologian yhdistymisessä omaksi kybertoimintaympäristön osa-alueekseen (Nikhat & Yusuf, 2020).

Silmälasit sisältävät jo kameroita ja ovat yleisessä myynnissä, ja kontaktilinsseihin pystytään liittämään kameroiden lisäksi koko ajan enemmän ominaisuuksia, kuten katseen suuntaa seuraava laserosoitin joka toimii mikroskooppisen pienillä optoelektronisilla komponenteilla, eli linssin elektroniikka muuttaa sähköä valoksi (Khaldi ym.), tai älykkäät anturijärjestelmät joiden avulla voidaan

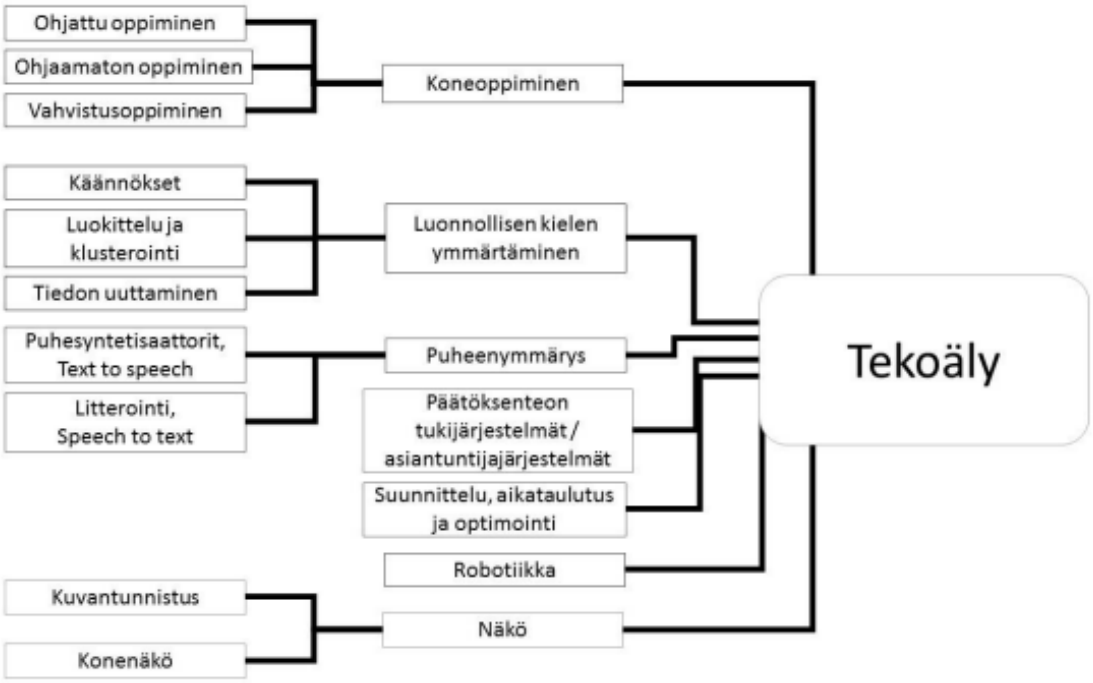
suorittaa silmädiagnostiikkaa (Kim ym., 2017). Kun tällaista kehitystä yhdistetään esim. Neuralinkin aivoimplanttikehitykseen (Neuralink, 2024) jossa henkilö pystyy ohjaamaan laitteita implantin avulla, ollaan jo hyvin lähellä miettimässä transhumanismia ja sen aiheuttamia mahdollisia uhkia. Myös proteesikehitys asettaa uusia haasteita, sillä jatkossa proteesit voivat olla hyvin monitoimisia laitteita suoraan ihmisen aina mukana olevana osana. Nämä liittyvät toistaiseksi eniten fyysisiin ja kyberuhkiin, mutta tulevaisuuden kehitystä tulee seurata.

Robotit ja robotiikka ovat oma osa-alueensa, joiden kehittyminen sitoutuu hyvin vahvasti tekoälyn käyttöön, kone- ja syväoppimiseen, sekä laskenta-/suorituskapasiteetin kasvuun, jotta roboteista saataisiin tarpeiden mukaan paitsi suorittavia, myös autonomisia, ja ympäristönsä kanssa aitoon ymmärtävään kommunikointiin ja konemuotoisiin aistihavaintoihin kykeneviä (Neittaanmäki ym., 2021, s. 89-91, 121-125). Tällaiset robotit ovat jo niin monimuotoisia kokonaisuuksia, että niiden aiheuttamat uhat tulee arvioida erikseen riippuen toimintaympäristöstä. Siinä missä tämän hetken imurirobotti voi lähettää kuvia, pohjapiirustukset, sekä käyttäjädataa, yksinkertaisimmillaan tulevaisuudessa robotit voivat kerätä ja käsitellä kaikkea niille syötettyä tai ympärillä tapahtuvaa huomattavasti monipuolisemmin.

5.1.1 Tekoäly

Tekoälyä on käsitelty laajasti jo tässä tutkimuksessa, sillä tällä hetkellä ei ole montaakaan uhkaa tai mahdollisuutta, tai kehittyvää teknologiaa, johon tekoäly ei jollain tavalla kytkeytyisi, tai voisi olla osana sen toimintojen kehittämisessä. Siihen liitettyjä termejä ja osa-alueita oli myös liikaa avattavaksi syvällisesti tässä tutkimuksessa, joten tässä kappaleessa avataan lähinnä lyhyesti tekoälyn osa-alueita tai ”haaroja”, sekä perinteisen ja generatiivisen tekoälyn eroja, jotta ymmärretään paremmin niiden aiheuttamat uhat, sekä niiden sisältämät mahdollisuudet.

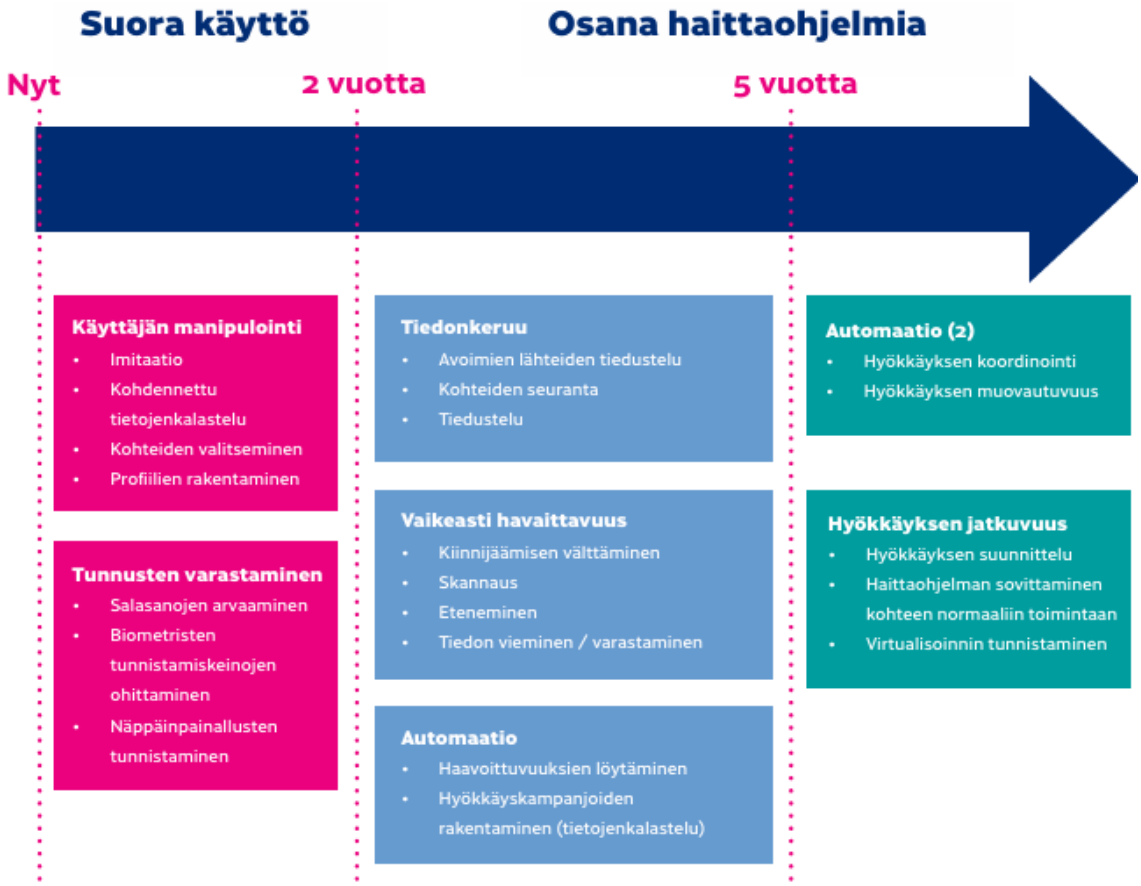
Tekoäly sisältää monia eri osa-alueita, jotka toimivat hieman eri periaatteilla ja kentillä. Näistä yleisimpiä ovat mm. koneoppiminen ja siihen liittyvä syväoppiminen, (luonnolliset) laajat kielimallit, robotiikka, syväoppiminen, neuroverkot/keinotekoiset hermoverkot, tietokonenäkö, puheentunnistus, asiantuntijajärjestelmät, parviäly, sumea logiikka jne. (Geeksforgeeks, 2024; Neittaanmäki ym., 2021, s. 20). Kenttä on siis hyvin laaja missä tekoälyä jo hyödynnetään. Neittaanmäen, Lehdon & Savosen verkkokirjassa ”*Yhteiskunnan digimurros*” (2021) kuvataan tekoälyn osa-alueita helposti käsitettävänä kaaviona (KUVIO 9).



KUVIO 9: Tekoälyn osa-alueet (Neittaanmäki ym., 2021, s. 88)

Tekoäly voidaan jakaa perinteiseen ja generatiiviseen tekoälyyn. Perinteinen tekoäly on reaktiivinen keskittyen sille syötetyn tiedon prosessointiin ja analysointiin voidakseen esim. tarjota ennusteita toteutumista ja sitä käytetään varsinkin toimintojen tehostamiseen. Generatiivinen tekoäly taas on kykenevä luomaan uusia asioita datamalleistaan ja sille syötetyistä tiedosta (Sengar ym., 2024).

Sekä tulevaisuuden uhat ja mahdollisuudet keskittyvät jo tutkimuksessa aiemmin läpikäytyjen uhkien ja mahdollisuuksien osalta tekoälyn laajan käyttöpotentiaalin ympärille, perinteisen tekoälyn tarjoamiin mahdollisuuksiin toimintojen tehostamisessa, ennustavien mallien luomisessa, syötetyn datan käsittelyssä ja kouluttamisessa riittävän laadukkaasti, sekä generatiivisen tekoälyn kyvyssä luoda ja kehittää uutta. Matti Aksela, Samuel Marchal ym. kuvaavat Traficomin raportissa ”*Tekoälyn mahdollistamat kyberhyökkäykset*” tekoälyn nostamiksi eduiksi mm. automatisoinnin joka nopeuttaa ja helpottaa hyökkäysten suorittamista, työkalujen tehostamisen niin mittakaavan kuin kohdentamisenkin kautta, hyökkäysten kattavuuden optimoinnin avulla sekä hyökkäysten kehittyneisyyden joka antaa kokonaan uusia kyvykkyyksiä hyökkääjille, ja tekee hyökkäyksistä hienostuneempia, vaikeasti havaittavampia, ja muokkautuvia (Aksela ym., 2022, s. 9-11). Raportissa arvioidaan lisäksi tekoälyn hyödyntämisen aikajanaa nyt ja tulevaisuudessa (KUVIO 10) jossa nähdään miten nykyisestä suorasta käytöstä tekoäly tullaan sitomaan osaksi haittaohjelmien toiminnallisuutta.



KUVIO 10: Tekoälyn mahdollistamien hyökkäysten aikajana (Aksela ym., 2022, s. 22)

5.1.2 Kvanttiteknologia

Kvanttiteknologian merkittävyys turvallisuudessa perustuu sen mahdollistamaan, nykyiseen verrattuna eksponentiaaliseen suorituskykyyn, ja fyysisiin sekä datan käsittelyn mahdollisuuksiin, joita ei ole sidottu nykyisten ratkaisujen rajoituksin. Josh Schneider ja Ian Smalley IBM:lta avaavat tätä verkkoartikkelissaan ”*What is quantum computing?*” (2024). Tieteenala on laaja ja monimutkainen, joten tässä tutkimuksessa keskityttiin vain siihen mitä vaikutusta sillä on kyberuhkien, sekä kyberturvallisuuden keinojen kannalta yleiseltä tasolta.

Outi-Marja Latvala käsittelee VTT:n julkaisussaan ”*Policy brief - Kvanttiturvalliset salausmenetelmät Suomessa*” miten kvanttitietokoneet tulevat mullistamaan ja tekemään hyödyttömäksi nykyiset kryptografiset ratkaisut, jotka perustuvat julkisen ja yksityisen avaimen algoritmeihin (asymmetrinen ja symmetrinen) ja ovat haavoittuvia Shorin tai Groverin algoritmeille joka kykenee laskemaan suurien lukujen tekijät erittäin tehokkaasti (Latvala ym., 2022, s. 2-9). Tätä varten on kehitetty, ja jatkuvasti kehitteillään erilaisia kvanttiturvallisia PQC-algoritmeja (post quantum algorithm) joiden salaustapaa vastaan kvanttitietokoneiden algoritmeista ei ole hyötyä. Nämä perustuvat sellaisiin matemaattisiin rakenteisiin, joilla on totutusta poikkeavia ominaisuuksia, kuten suurempia avaimia, allekirjoituksia, tai salatekstejä. Haasteena näissä on, että ne eivät

pääasiallisesti ole suoraan liitettävissä nykyisiin järjestelmiin, tietoverkkoihin ja protokolliin (Latvala, 2022, s. 2-9.). Eri maat ja standardit ovat jo huomioineet kvanttiteknologian uhat salaukselle, ja ovat eri vaiheissa prosesseja salausalgoritmien valinnassa, mutta koska haavoittuvuuksia ei ole vielä pystytty kattavasti selvittämään on markkinoilla useita ratkaisuja (Latvala, 2022, s. 3-5).

Siinä missä kvanttiteknologia aiheuttaa uhkia se mahdollistaa myös suojauskeinoja ja teknologiaa, jotka eivät aiemmin ole olleet mahdollisia, ja siitä tulee olemaan suurta hyötyä mm. tekoälyn ja koneoppimisen kehittämisessä ja mahdollistamisessa (Latvala, 2022, s. 6). Sen avulla pystytään tehostamaan olemassa olevia ratkaisuja, suojaamaan dataa ja esimerkiksi havaitsemaan hyökkääjiä tehokkaasti kloonaamattomuusteorian avulla (Faruk ym., 2022, s. 7; Helsingius, 2017, s. 6.).

5.1.3 IoT

IoT, jossa laitteet kommunikoivat internetin välityksellä lähti kehittymään 2010-luvun alussa merkittävästi, vaikka termi keksittiinkin jo 1999 Kevin Ashtonin toimesta (Neittaanmäki ym., 2021, s. 103). IoT -laitteet voivat olla, joko yksipuolisesti vastaanottavia, tai kaksisuuntaisia älylaitteita, ja ne voivat myös verkottua keskenään. Vuonna 2021 maailmassa oli yli 10 miljardia IoT -laitetta. Vuonna 2025 niiden arvioidaan tuottavan n. 73,1 ZB (zetabitti) dataa. Vuonna 2030 laitteita arvioidaan olevan yli 25,4 miljardia, eli trendi älylaitteisiin on voimakkaasti kehittyvä, kuten Bojan Jovanovic (2024) IoT -statistiikka käsittelevässä verkkoartikkelissaan kirjoittaa. Voimakkaasti kasvavan määrän lisäksi laitteiden kehitys kulkee käsi kädessä muiden kehittyvien teknologioiden osana, kuten tekoälyn,

Myös Neittaanmäki, Lehto & Savonen (2021, s. 103-104) nostavat IoT:n merkittävyyden, sillä ne ovat nykyisin hyvin laajasti käytössä elämässämme ja palveluissa yksityisistä käyttäjistä teollisuuden kautta sotilaskäyttöön.

IoT:iin liittyy monia kyberuhkia ja huolia. Jovanovic (2024) listaa näistä merkittäviksi huomioiksi mm. IoT -laitteita hyväksikäyttämällä tehtyjen haittaohjelmahyökkäysten kasvun 300 %:lla vuosien 2018-2019 välillä, tietosuojahuolet (laitteiden keräämä data, sen käyttö, sekä suojaaminen ulottaen tämän myös toimitusketjuun), hyökkäysten havaitsemattomuuden organisaatioissa (48% ei havaitse IoT -hyökkäyksiä verkossaan), sekä että moniin laitteisiin ei lähtökohtaisesti ole rakennettu mitään suojausta tukevia ominaisuuksia. Tätä pyritään ohjaamaan EU:ssa regulaatiolla. IoT -laitteita käytetään myös hyvin laajasti hyväksi hajautetuissa palvelunestohyökkäyksissä (DDoS) joissa huonosti suojattujen laitteiden verkkoja käytetään hyväksi bottiverkkona. Kun huomioidaan olemassa olevien laitteiden määrä ja sen kasvu tämä on tulevaisuudessa uhkana entistä merkittävämpi.

5.1.4 Lohkoketjut

Neittaanmäki, Lehto & Savonen kuvaavat lohkoketjua hajautetuksi tilikirjaksi tai tietokannaksi, jonka loppuun voi lisätä dataa, mutta aiempia osia ei voi muokata

tehden siitä näin turvallisen (2021, s. 108). Guo & Yu (2022) kuvaavat artikkelissaan "*A survey on blockchain technology and its security*" lohkoketjujen turvallisuuteen liittyviksi ominaisuuksiksi autonomisuuden, eheyden ja muuttumattomuuden tukemisen, vikasietoisuuden ja anonyymiteetin, sekä tarkastettavuuden ja läpinäkyvyyden. Ominaisuuksistaan johtuen lohkoketjuja käytetään paljon kryptovaluutan käsittelyssä ja yleisesti pankkialalla eri palveluiden toteuttamisessa, sopimuksissa, sekä mm. autentikoinnissa (Neittaanmäki ym., 2021, s. 107-108). Lohkoketjuihin kohdistuvat yleisimmät kyberuhkat liittyivät Guon ja Yu:n (2022) tutkimuksen mukaan 51%:ssa tapauksia haavoittuvuuksiin, rikolliseen toimintaan, sekä yksityisten avainten turvallisuuteen.

5.1.5 6G

6G on kehitteillä oleva, älykäs langaton verkko, joka pystyy tarjoamaan nopeampaa tiedonsiirtoa, toiminnan luotettavuutta, alhaisempia viiveitä ja tehokkaampaa laitteiden välistä yhdistettävyyttä (Pathak ym., 2023, s. 1-2; Porambage ym., 2021, s. 1-3)

6G pystyisi suunnitelmien mukaan hyödyntämään tehokkaasti erilaisia olemassa olevia sekä kehittyviä teknologioita, kuten mm. kvanttiteknologiaa, tekoälyä ja siihen liittyvää koneoppimista, lohkoketjuja ja -teknologiaa, terahertsitekniikkaa, (bio)nanoteknologiaa & -kommunikaatiota, sekä tiedonsiirtoa näkyvällä valolla (VLC) (Pathak ym., 2023; Poramabge ym., 2021, s. 1-6; Ylianttila ym., 2020, s. 5-26). 6G tulee siis olemaan palvelualusta monille kehittyville teknologioille.

6G:n osalta ei voida vielä tarkasti määritellä mitä sen turvallisuuden osalta tulisi ottaa kaikkiaan huomioon, koska verkkoratkaisu on vasta kehitteillä, ja kirjallisuutta aiheesta, sekä tietoa on rajatusti. On arvioitu, että verkko voitaisiin ottaa kuluttajakäyttöön vuonna 2030 (Porambage ym., 2021, s. 1-3; Ylianttila ym., 2020, s. 5-26)

Verkkoon kohdistuvia uhkia ei pystytä myöskään määrittelemään tarkasti, mutta ne liittyvät paitsi em. teknologioihin myös fyysiseen turvallisuuteen, sekä varsinkin näiden hybridiuhkiin

5.2 Massadata ja tietoaltaat

Massadatalla (big data) ja tietoaltailla tarkoitetaan niin massiivisia ja monimutkaisia kokonaisuuksia, että niiden tehokas käsittely ja analysointi tarvitsee kehittyvää teknologiaa, kuten tekoälyä ja kvanttiteknologiaa (Euroopan parlamentti, 2021, Euroopan komissio, 2024 ; Neittaanmäki ym., 2021, s. 77-85). Datan käsittelyn vaatimuksia tulevaisuudessa on huomioitu myös EU -tason lainsäädännössä. Data halutaan vapaasti ja tehokkaasti saataville EU :n sisämarkkinoille ja avainalojen välillä kuitenkin tietosuojasta ja turvallisuudesta huolehtien. Tätä ohjaavat mm. Datahallintasäädös sekä tekoälysäädös. (Euroopan parlamentin ja neuvoston asetus 2022/868; Euroopan komissio, 2024).

5.3 Ihmiset

Ihminen kyberuhkien aiheuttajana, kohteena ja kyberhyökkäysten mahdollistajana on otettava erikseen esiin, koska se toistui merkittävänä tekijänä kyberuhkia käsiteltäessä riippumatta tutkitusta materiaalista. Ei ole myöskään mitään merkkejä siitä, että tämä olisi poistumassa tai vähenemässä, päinvastoin, kuten VNK kyberturvallisuustrategiassaan, sekä ENISA raportissaan kuvaavat (ENISA, 2023, s ;VNK, 2024, s. 13-14).

Hyvin moniin kyberhyökkäyksiin liittyy ihmisen toiminta, näistä kirjallisuuskatsauksessa on nostettu esiin tahalliset ja tahattomat virheet eri toiminnoissa on sitten kyse esim. sähköpostin käytöstä, ohjelmoinnista tai IT-/OT -tekniikan hallinnoinnista. Tämän lisäksi mm. sosiaalinen manipulointi, tietojen kalastelu ja petokset tuovat oman lisänsä, eikä vain omien toimijoiden, vaan myös toimitusketjujen kautta.

Nyt ja tulevaisuudessa inhimillisten tekijöiden ja varsinkin osaamisen ja tietoisuuden puutteiden arvioidaan tulevan aina olemaan merkittävä uhka, mutta myös merkittävä suojauskeino ja mahdollisuus koulutuksen, osaamisen ja tietoisuuden kautta.

5.4 Hybridiuhat

Tutkimuksen materiaaleissa yhdistyy myös usein tekoälyn ja siihen liittyvän koneoppimisen, kvanttiteknologian ja 6G:n yhdessä aiheuttamat uhat ja haasteet, joiden kaikkia mahdollisuuksia, ulottuvuuksia ja merkittävyyttä emme vielä pysty hahmottamaan kunnolla, myös avaruusteknologian hallinnoinnin tuodessa omat ulottuvuutensa. Tästä syystä on tärkeää seurata kaikkien näiden teknologioiden kehittymistä ajantasaisten uhkamallien luomiseksi huomioiden samalla, että vanhat uhat eivät usein poistu mihinkään.

5.5 Sähkönjakelu ja akkuteknologia

Digitaalisessa maailmassa harva asia on tärkeämpi kuin sähkö. Sen riittävyyteen, saatavuuteen, tuotantokeinoihin ja käytettävyyteen kohdistuu jatkuva mielenkiinto, ja sähkön saatavuus liittyy erottamattomasti jatkuvuudenhallintaan perusvaatimuksena.

International Energy Agency (IEA) arvioi vuoden 2024 ”*Electricity 2024 – Analysis and forecast to 2026*”, että maailman kokonaissähkönkulutus kasvaa joka vuosi keskimäärin 3,4%. Raportin mukaan mm. palvelinkeskukset, tekoäly, sekä kryptovaluutan louhinta käyttävät merkittävästi sähköä, ja palvelinkeskusten vuosittainen kulutus joka nyt on 460TTHh Terawattituntia) voi kohota jopa 1000TWh vuonna 2026. (International Energy Agency [IEA], 2024, s. 8, 16).

Vuonna 2024 geopoliittinen tilanne on epävakaa, ja tämä aiheuttaa omat huolensa sähkön saatavuuteen. Vuonna 2022 Fingrid ilmoitti, että Suomi ei ole riippuvainen Venäjältä tuodusta sähköstä, vaan on Olkiluoto 3 ja lisääntyvän tuulivoiman avulla energiaomavarainen 2024 mennessä (Fingrid, 2022). Raportissaan sähkön riittävyydestä 2024–2030 aikavälillä Fingrid kuitenkin huomioi lisääntyvän energiantarpeen niin sähköistyvien teollisuuden, liikenteen, vedyntuotannon kuin lämmityksen tarpeiden vuoksi kasvavan 50% vuoteen 2030 mennessä (Fingrid, 2023, s. 9-10). Raportissa huomioitiin aikaisemman mukaisesti, että perustilanteessa sähkön riittävyys on hyvä, mutta merkittävissä vikatilanteissa riski tehovajeesta kasvaa. (Fingrid, 2023, s. 16-20).

Sähkönjakelun häiriöt voivat olla siis haaste tarpeiden kasvaessa, kun yhdistetään sekä Fingridin raportin tarpeet, sekä IEA:n huomiot kehittyvien teknologioiden ja palvelinkeskusten tarpeista.

Organisaatioiden jatkuvuudesta puhuttaessa näiden tulisi valmistautua mahdollisiin sähkönsyötön häiriöihin. Keskeytymätön virransyöttö (UPS, uniterruptible power supply) on jo käytössä monilla organisaatioilla kriittisiin järjestelmiin ja toimintoihin liittyen, mutta niiden tarkoitus on turvata lyhytaikaiset katkokset. Pidempiaikaisiin katkoksiin organisaatioilla voi olla varavoimajärjestelmiä. Tässä tulevaisuuden kannalta mielenkiintoinen asia on mm. tämänhetkinen akkuteknologian nopea kehitys. Energiantuotantoa ohjataan koko ajan enemmän uusiutuvien energiamuotojen suuntaan luonnonvarojen säästämiseksi. Näissä ongelmana on saatavuuden vaihtelevuus (esim. aurinko- ja tuulivoima), jolloin osan aikaa syntyy ylituotantoa, ja ajoittain tuotannossa on vajetta. Tällä hetkellä kehitetään tehotiheydeltään parempia ja luonnonvaroja säästävämpiä akkuja, jotka tulevat enemmän myös kuluttajien käyttöön tulevaisuudessa.

Julia Amici ym. esittivät 2022 EU:n ”*Battery 2030+*” -tutkimusprojektia tukevassa tutkimuksessaan laajan etenemissuunnitelman mitä akkuteknologioiden osalta tulee tapahtumaan. Suunnitelma alleviivasi kokonaisvaltaista kehitystarvetta, sekä erilaisia osa-alueita ja niiden haasteita, mutta myös kehityksen merkittävyyttä infrastruktuureille kaikilla tasoilla (Amici ym. 2022) Käytännössä akut voivat olla kuitenkin omia älykkäitä ”pienoisvoimaloita” joiden tehokkuus, kestävyys, ja itsenäinen kapasiteetti toimia ja korjautua ovat ylivoimaisia nykyisiin nähden.

Akkujen kapasiteetti siis kasvaa, ja niiden merkitys uusiutuvien energiantuottomuotojen tukijana ja sähkökulutuksen tasausmetodina muuttuu koko ajan merkittävämmäksi myös organisaatioissa tulevaisuudessa jatkuvuudenhallinnan tukena.

5.6 Yhteenveto

Yhteenvetona voi todeta, että kyberturvallisuuskenttä on hyvin laaja, monimutkainen, ja se on kehittymässä jatkuvasti vaativammaksi. Teknologia ottaa tällä hetkellä harppauksia, joiden vaikutuksista ja verkottumisesta muiden osa-alueiden kanssa meillä ei ole aina selkeää käsitystä. Samalla kyberrikollisuus on

kasvussa, helpompaa, ja ihmisten kyberturvallisuusosaaminen ei ole sellaisella tasolla, että useinkaan pystyttäisiin vastaamaan olemassa oleviin ja nouseviin kyberuhkiin, ja näiden aiheuttamat kustannukset maailmantaloudelle ovat koko ajan kasvussa. Suurimpana vaikuttajana tässä on ihminen – jos osaamista pystytään kasvattamaan, myös negatiivisia vaikutuksia pystytään merkittävästi pienentämään.

Tämän lisäksi on huomioitava, että uhat verkottuvat toistensa kanssa, ja niiden muodostamista kokonaisuhkista ei ole vielä selvää kuvaa tulevaisuuttaa ajatellen. Tällä hetkellä voidaan keskittyä lähitulevaisuuden haasteisiin ja niiden ratkaisemiseen niin regulaation, standardien hyvien käytäntöjen, asiantuntijaosaamisen, kuin teknologioiden ja tutkimisen avulla. Oman osansa jatkuvuudenhallintaan tuovat kriittiseen infrastruktuuriin ja sen mahdollisiin häiriöihin kohdistuvat riskit mm. sähkön osalta.

Huolimatta merkittävistä riskeistä, joita nousevat teknologiat aiheuttavat organisaatioille niiden jatkuvuutta silmälläpitäen materiaaleissa nousi esiin myös, että teknologinen kehitys myös mahdollistaa uhkien tunnistamista ja niiltä suojautumista samalla tavalla.

6 TUTKIMUSMENETELMÄT

Tutkimus oli sekä kirjallisuuskatsauksen, että empiirisen tutkimuksen keinoin toteutettava laadullinen tutkielma, jossa tieteellisen- ja asiantuntija-aineiston avulla selvitettiin niin nykytilannetta kuin tulevaisuuden haasteita ja uhkia, sekä kehitystarpeita.

Tutkielmaa tuettiin laadullisen tutkimuksen avulla anonyymisti verkossa suoritettavalla kyselyllä, jolla voitiin selvittää asiantuntijoiden näkemyksiä tutkimuskysymyksiin liittyen. Tämän lisäksi suoritettiin neljä puolistrukturoitua asiantuntijahaastatteluita, joiden avulla reflektoitiin tutkielmaa ja sen löydöksiä, saatiin syvennettyä laadullista ymmärrystä nykytilanteesta, sekä lisänäkemystä kehittämistarpeista.

6.1 Kirjallisuuskatsaus

Tietoa haettiin kirjallisuuskatsauksen kautta riittävän teoreettisen pohjatiedon hankkimiseen, sekä kyselyiden ja haastatteluiden vertaisarviointiin. Koska saatavilla oli rajallisesti tieteellistä tutkimustietoa kyberturvallisuuden ja jatkuvuudenhallinnan keskinäisestä vuorovaikutuksesta lähdemateriaaleina käytettiin myös esimerkiksi lakeja, standardeja, valtionhallinnon ohjeistuksia, sekä asiantuntija-artikkeleita ja -blogeja, joita vertailtiin toisiinsa tiedon luotettavuuden varmistamiseksi, jotta voitiin vähentää yksittäisten henkilöiden näkemysten merkittävyyttä.

Oli selkeästi todettavissa, että kybermaailman uhkiin, sekä kyberturvallisuuden hallintaan löytyy todella paljon ja monipuolisesti kirjallista materiaalia, mutta jatkuvan nopean kehityksen vuoksi tieteelliset tutkimukset ovat usein jo myöhässä, eivätkä kuvasta aina niin hyvin nykyisiä trendejä, joita tässä tutkielmassa pyrittiin käsittelemään. Tästä syystä huomattavan suuri osa kirjallisuuskatsauksen materiaaleista oli eri asiantuntijalähteistä kerättyä.

Jatkuvuudenhallinnan puolella materiaalin saatavuus ja määrä taas olivat rajatumpia. Tämä johtui luonnollisesta syystä, että jatkuvuudenhallinta itse prosessina on rajatumpi kuin kybertoimintaympäristö, eikä niin monimutkainen omana kokonaisuutenaan. Tässä mielessä materiaalin vähäisempi määrä ei ollut yllättävä tulos.

Organisaatioiden jatkuvuudenhallintaan löytyi ohjeistusta mm. Kyberturvallisuuskeskukselta, sekä palveluina auditointilaitoksilta sertifiointien muodossa, mutta tutkimustuloksia ja näitä kahta osa-aluetta koskevaa yhteistarkastelua organisaatioihin kohdistuen oli vähän.

Kirjallisuuskatsauksen analyysissa keskityttiin vertailemaan tehtyjä löydöksiä materiaaleista, ja vetämään näistä linjaavia johtopäätöksiä.

6.2 Empiirisen tutkimusaineiston kerääminen

Empiirinen tutkimusaineisto muodosti vertailuaineiston tutkimuksen tiedonkeruusta aiheen tarkastelun tueksi. Aineisto kerättiin useammilla metodeilla. Näitä olivat sekä kysely sisältäen määrällisen ja laadullisen osuuden, että laadulliset puolistrukturoidut asiantuntijahaastattelut.

Tutkimuksen aihealueen pohjalta tehtiin Likert-asteikolla suoritettava viisiportainen kysely, joka sisälsi sekä määrällisen, että laadullisen elementin. Tämän kautta kerättiin tietoa asiantuntijanäkemyksistä kohdistuen tutkimuksen aihealueisiin ja tutkimuskysymyksiin kohdistuen organisaatioiden nykytilanteeseen ja koettuun kyvykkyyteen.

6.2.1 Kysely

Kysely tehtiin Likert-asteikolla, joka on Rensis Likertin 1932 kehittämä menetelmä asenteiden, mielipiteiden, käyttäytymisen ja mieltymysten mittaamiseen (Likert, 1932, s. 5-53) ja on eräs käytetyimmistä ja tunnetuimmista menetelmistä kerätä jäsenneltyä tietoa vertailukelpoisessa ja mitattavassa muodossa. Likert-asteikolla suljetuilla kysymyksillä on aina vastausvaihtoehtoina kaksi ääripäätä, ja arviointiasteikkojen portaiden määrä voi vaihdella tutkimuksen mukaan.

Menetelmäksi valittiin Likertin viisiportainen asteikko, koska menetelmän ja portaikon katsottiin sopivan aihealueeseen liittyvän analysoitavan tiedon saamiseen käytettäessä suljettuja kysymyksiä. Viisiportaisessa asteikossa on ääripäiden lisäksi aina keskellä neutraalimpi vaihtoehto, joka haluttiin tutkimukseen mukaan monipuolisuuden ja lisäämiseksi, sekä, että vastaajia ei pakotettaisi valitsemaan toiseen ääripäähän painottuvaa vastausta, jos tilanne koettiin neutraaliksi. Vastausvaihtoehtoina kysymyksiin oli kysymyksestä tai väittämästä riippuen jompikumpi alla olevista vaihtoehdoista (TAULUKKO 2). Tämän lisäksi molemmissa oli mahdollisuus ohittaa kysymys tai väittämä, jos henkilö koki, että ei jostain syystä voi vastata kohtaan. Kysymyspatteristo löytyy liitteestä 2.

TAULUKKO 2: Likert-kysely vastausvaihtoehdot

Kysymysten vastausvaihtoehdot (Osio 1)	Väittämien vastausvaihtoehdot (Osiot 2 ja 3)
Erittäin huonosti	Täysin eri mieltä
Huonosti	Eri mieltä
Kohtuullisesti	Ei samaa eikä eri mieltä
Hyvin	Samaa mieltä
Erittäin hyvin	Täysin samaa mieltä
Ohita kysymys	Ohita väittämä

Kysely jakautui kyselyn esittelyyn, organisaatiotyypin määrittämiseen, sekä neljään varsinaiseen kyselyosioon (TAULUKKO 3).

TAULUKKO 3: Kyselyn rakenne ja aihealueet

Osio
Kyselyn esittely
Organisaatiotyypin valinta
1. Organisaatioiden jatkuvuudenhallintaan liittyvä valmistautuminen ja suunnittelu keskittyen kyberturvallisuuteen yleisesti.
2. Organisaatioiden koettu valmius vastata vakaviin jatkuvuuteen vaikuttaviin kyberuhkiin, -poikkeamiin ja -hyökkäyksiin.
3. Organisaatioiden kyberturvallisuuteen kohdistetut metodit, prosessit ja työkalut.
4. Avoimet kysymykset ja vapaa sana

Esittelyssä kerrottiin kyselyn tekijästä ja tarkoituksesta, aiheesta, kyselyn anonyymiudesta, tietojen käsittelystä, vapaaehtoisuudesta, kyselyn voimassaoloajasta sekä kuinka kauan vastaaminen arviolta kestää. Tämän lisäksi esittelyssä kerrottiin kyselyn rakenteesta, ja annettiin alustavat ohjeita kyselyyn vastaamiseen. Kyselyn vastaajille kerrottiin toivotusta vastaajien kompetenssista: ”*Kysely on kohdistettu henkilöille, joilla on suoraan tai välillisesti kokemusta, tietoa ja ymmärrystä organisaatioiden jatkuvuudenhallinnasta ja sen keinoista, sekä kyberturvallisuudesta osana jatkuvuudenhallintaa*.” Tällä haluttiin rajata vastaajaprofiilia asiantuntijoihin, joita tutkimusaihe koskettaa ja joilla voi olla syväosaamista tutkimusalueeseen liittyen. Kyselyn esittelyteksti löytyy liitteestä 1.

Kyselyssä pyydettiin ensin määrittämään organisaatiotyyppi, koska tiedostettiin jo ennakolta kirjallisuuskatsauksen perusteella, että näissä voi olla eroavaisuuksia, ja haluttiin selvittää näkyvätkö nämä myös kyselyvastauksissa. Vaihtoehtoina olivat pienet / keskisuuret organisaatiot, tai suuret / kriittiseen infrastruktuuriin kuuluvat organisaatiot. Kriittiseen infraan kuuluvia organisaatioita ei haluttu eritellä omakseen, koska ei haluttu vastaajien joutuvan huolehtimaan vastausten sensitiivisyydestä. Samasta syystä tarjottiin lisäksi tarjottiin vaihtoehtona vastata organisaatiokenttään yleisesti, koska haluttiin vähentää vastaajien huolta siitä voitaisiinko anonymiteetista huolimatta vastaukset kohdentaa tietyntyyppiseen organisaatioon. Tämä asia huomioitiin myös esittelytekstissä. Tässä hyväksyttiin siis suurempi epätarkkuus organisaatiokentittäin vastausten määrän kasvattamiseksi.

Seuraavat osiot sisälsivät varsinaiset kysymykset. Kolme ensimmäistä näistä sisälsi suljettuja kysymyksiä Likertin asteikolla arvioituna, ja neljäs sisälsi avoimia kysymyksiä aihealueeseen liittyen (TAULUKKO 3).

Kysely sisälsi kuusi (6) suljettua kysymystä (Osio 1), Neljätoista (14) väittämää (Osiot 2 ja 3), sekä 3 avointa kysymystä (Osio 4) joiden jälkeen oli vielä vapaa sana. Kysymykset ja väittämät käsittelivät aihealuetta eri näkökulmista kattaen niin suojattavan omaisuuden tunnistamista ja hallintaa, dokumentaatiota, prosesseja, resurssointia, harjoittelua, kuin ennakoivaa varautumistakin.

Kysely suoritettiin anonyymina verkkokyselynä käyttäen Jyväskylän Yliopiston tarjoamaan Webropol-ohjelmistoa. Tämän kautta henkilöille voitiin jakaa halutuilla alustoilla avoin linkki anonyymiin kyselyyn.

Likert-asteikko sopi parhaiten analysoitavan materiaalin menetelmäksi tutkimuksessa, mutta mietittiin, olisiko pitänyt käyttää joko kuusiportaista asteikkoa jotta vältettäisiin väittämissä täysin neutraali vaihtoehto. Tämä vältettiin

kysymyksissä käyttämällä keskimmäisenä vaihtoehtona termiä ”kohtuullisesti”, mutta sana ei itsessään ole täysin neutraali, joten on mietittävä ohjasiko tämä vastauksia positiivisempaan suuntaan.

Kysely jaettiin seuraavissa kanavissa: LinkedInin suljetuissa turvallisuuteen ja jatkuvuudenhallintaan liittyvissä ryhmissä (kaksi ryhmää), muissa asiantuntijaryhmissä, joissa tutkija oli osallinen, sekä lisäksi myös oman LinkedIn -profiilin kautta ja henkilökohtaisia verkkoja käyttäen. Ryhmiä ei nimetä tutkimuksessa luottamuksellisuuden vuoksi. Kyselyn osalta tiedostettiin, että koska se oli tiettyjen kanavien kautta nähtävissä kaikille, oli väärinkäytön mahdollisuus olemassa (bottivastaaminen, häirintä, valheelliset vastaukset ohjaamaan kyselyn tuloksia jne.). Tämä tiedostettiin ja varauduttiin arvioimaan jokainen vastaus erikseen, jotta havaittaisiin mahdolliset indikaattorit, jotka viittaisivat muihin kuin asiantuntijavastauksiin ja voitaisiin perustellusti osoittaa mitkä vastaukset on otettu pois ja millä perustein, mutta, että vastaukset kuitenkin ovat nähtävillä raakadatasta. Koska kyselyssä haluttiin eritellä, minkälaisten organisaatioiden osalta kyselyyn vastataan (pienet- ja keskisuuret, suuret / kriittiseen infrastruktuuriin liittyvät organisaatiot, vai yleisesti) rajattiin vastausmahdollisuudet Webropolin toiminnallisuuden avulla kolmeen samalta selaimelta. Tämä oli mahdollista ohittaa tyhjentämällä selaimen välimuisti, tai vastaamalla toisen selaimen kautta, mutta toimenpiteen katsottiin antavan kuitenkin kontrollia vastausmääriin.

Kyselyn tulosten analysoinnissa käytettiin teemoittelua, joka Kirsi Juhilan (2021) mukaan on laadullisen tutkimuksen sisällönanalyysin muoto, jonka avulla tunnistetaan tutkimusongelman kannalta olennaiset aiheet, sekä pystytään jäsentelemään saatu aineisto (Eskola & Suoranta, 2008, s. 174-180; Tuomi & Sarajärvi, 2018). Teemoittelu huomioitiin kyselyä luotaessa, kun eri osa-alueet jaoteltiin aihealueittain (TAULUKKO 3). Näiden avulla kysymyksiä kohdennettiin valmistautumiseen ja suunnitteluun (osio 1), koettuihin valmiuksiin (osio 2), sekä metodeihin, prosesseihin ja työkaluihin (osio 3). Tämän lisäksi aihealueiden sisällä käytettiin teemoittelua jakamalla kysymyksiä koskemaan nykyistä tilannetta vs. ennakointia, resursseja ja alihankintaketjujen huomiointia. Kysymykset teemoiteltiin myös verraten niitä tutkimuksen alakysymyksiin (TAULUKKO 4). Kyselyn avulla haluttiin keskittyä selvittämään organisaatioiden nykytilannetta uhkien tunnistamisen ja niihin vastaavien kyvykkyyksien puolesta, koska niistä oli saatavilla vähiten tietoa kirjallisuuskatsauksen avulla.

Osio 1 keskittyi tutkimuksen alakysymykseen b. ja osiot 2 ja 3 alakysymykseen c. Avoimilla kysymyksillä (osio 4) haluttiin vielä lisätietoa asiantuntijoilta merkittävimmistä uhkista (kysymys 22.), sekä tehostamiskeinoista (kysymykset 21. ja 23.) joita käsitellään kappaleen yhteenvetoanalyysissa.

TAULUKKO 4: Kyselyn kysymysten teemoittelu tutkimuskysymyksiin verrattuna

Kyselyn kysymykset		**Tutkimuksen alakysymykset**			
		a.	**b.**	**c.**	**d.**
1.	**Tämän osion kysymykset kohdistuvat organisaatioiden jatkuvuudenhallintaan liittyvään valmistautumiseen ja suunnitteluun keskittyen kyberturvallisuuteen.**				
1.	Kuinka hyvin koette organisaatioiden tunnistaneen näiden kriittiset suojattavat toiminnot, omaisuuden (assets) ja resurssit?		x		
2.	Kuinka hyvin kyberturvallisuus ja sen keinot on mielestänne huomioitu kokonaisuudessaan osana organisaatioiden jatkuvuudenhallintaa?		x		
3.	Kuinka hyvin koette organisaatioiden tunnistaneen kyberturvallisuusriskit jotka voivat uhata liiketoiminnan jatkuvuutta?		x		
4.	Kuinka hyvin koette organisaatioiden varanneen riittävät henkilöresurssit ja budjetin kyberturvallisuudesta huolehtimiseen osana jatkuvuudenhallintaansa?		x		
5.	Kuinka hyvin koette organisaatioiden huomioineen toimitus- ja alihankintaketjujen aiheuttamat riskit jatkuvuudenhallinnassa kyberturvallisuuden kannalta?		x		
6.	Kuinka hyvin koette organisaatioiden tunnistavan nousevat ja uudet jatkuvuuteen vaikuttavat kyberuhat ja varautuvan niiltä suojautumiseen ennakoivasti suunnittelussaan?		x		
2.	**Tämän osion väittämät käsittelevät organisaatioiden koettua valmiutta vastata vakaviin jatkuvuuteen vaikuttaviin kyberuhkiin, -poikkeamiin ja -hyökkäyksiin.**				
7.	Organisaatioiden kyberturvallisuuspolitiikka ja muun aihealuetta ohjaava dokumentaatio, sekä toipumis- ja jatkuvuussuunnitelmat tukevat jatkuvuudenhallintaa riittävällä tasolla:			x	
8.	Organisaatiot pystyvät palautumaan vakavista jatkuvuuteen vaikuttavista kyberhyökkäyksistä ilman merkittäviä vaikutuksia niiden toiminnoille:			x	
9.	Organisaatiot pystyvät reagoimaan kyberhyökkäyksiin riittävän nopeasti siten, että niillä ei ole merkittävää vaikutusta kriittisiin toimintoihin:			x	
10.	Organisaatiot ovat varautuneet toimitus- ja hankintaketjujen kautta organisaatioon kohdistuviin jatkuvuuteen vaikuttaviin hyökkäyksiin ja riskeihin riittävällä tasolla:			x	
11.	Organisaatioiden valmiudet vastata uusiin ja nouseviin kyberuhkiin ovat riittävällä tasolla:			x	
12.	Organisaatioilla on käytössään nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin nähden ajantasaiset prosessit ja ohjeistukset joita päivitetään säännöllisesti uhkakuvien mukaisesti.			x	
3.	**Tämän osion väittämät käsittelevät organisaatioiden kyberturvallisuuteen kohdistettuja metodeja, prosesseja ja työkaluja.**				
13.	Organisaatioiden kyberturvallisuustoimenpiteet ovat kokonaisuutena tarkastellen riittävät suojaamaan organisaatiota uusimmilta uhkilta ja haavoittuvuuksilta.			x	
14.	Organisaatioilla on käytössään riittävät tekniset keinot, valmiudet ja työkalut vastata nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin.			x	
15.	Organisaatiot suorittavat harjoituksia ja testaavat kyberturvallisuuttaan riittävästi huolehtiakseen kriittisten resurssiensa suojaamisesta.			x	
16.	Testauksissa ja harjoituksissa huomioidaan tämän hetken merkittävimmät, sekä nousevat organisaatioihin kohdistuvat kyberuhat.			x	
17.	Organisaatioiden kriisi- poikkeustilanneviestintä kyberturvallisuuspoikkeamiin liittyen on riittävän tehokasta ja saavuttaa kaikki tarvittavat osapuolet riittävällä tasolla.			x	
18.	Organisaatiot tarjoavat riittävästi säännöllistä koulutusta työntekijöilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan jatkuvuudenhallinnassa.			x	
19.	Organisaatiot tarjoavat riittävästi säännöllistä koulutusta toimittajilleen ja alihankkijoilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan organisaation jatkuvuudenhallinnassa.			x	
4.	**Tässä osiossa on avoimia kysymyksiä joilla tarkennetaan aikaisempiin osioihin liittyviä aihealueita. Vastaaminen on vapaaehtoista, mutta auttaa tutkimuksen aihealueiden käsittelyn ja tutkimuksen syventämisessä**				
20.	Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta?				x
21.	Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne.	x			
22.	Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan?				x
23.	Vapaa sana. Voitte laittaa tähän ajatuksianne ja palautetta kyselyn aihealueeseen ja tutkimusaiheeseen liittyen.	x	x	x	x

Tulosten analysoinnissa käytettiin tilastollisista menetelmistä keskilukujen laskentaa sisältäen keskiarvon (keskimääräinen arvo), mediaanin (keskimmäinen

arvo) ja moodin (tyypillisin arvo) (Tilastokeskus, 2024). Työkaluna laskennassa käytettiin nettilaskuria (Laskurix, 2024). Tutkimuksen tavoitteena ei ollut tehdä laajaa ja syväluotaavaa tilastollista analyysia. Menetelmää käytettiin tukemaan kvalitatiivista tutkimusta pyrittäessä ymmärtämään trendejä ja suuntauksia, joita organisaatioissa tunnistettiin kokonaistilanteen ymmärtämiseksi ja tehostamiskeinojen kohdistamiseksi.

6.2.2 Haastattelut

Haastattelut ovat paljon käytetty tapa tuottaa laadullista tutkimusaineistoa, kun tavoitteena on tuottaa tietoa tutkimusongelmaan vastaamiseksi (Hyvärinen. Suoninen & Vuori. 2021)

Haastattelun muotoja ovat strukturoitu, puolistrukturoitu ja vähän strukturoitu. Strukturoidussa haastattelussa minimoidaan variaatio vastauksissa ennalta määritetyillä vastausvaihtoehdoilla, ja halutaan minimoida haastattelijan vaikutus ennalta määritetyillä kysymyksillä. Puolistrukturoidussa haastattelussa kysymykset laaditaan ennakkoon, mutta haastateltavat saavat vastata niihin omin sanoin, myös lisäkysymykset ja tarkennukset ovat mahdollisia. Vähän strukturoidussa haastattelussa taas sekä kysymykset että vastaukset voivat olla vielä avoimempia ja keskustelunomaisia (Hyvärinen, Suoninen & Vuori, 2021).

Haastattelumuodoksi tutkimukseen valittiin asiantuntijahaastattelu puolistrukturoidulla lähestymistavalla. Haastateltavina olleille asiantuntijoille lähetettiin etukäteen tutkimusaiheeseen pohjautuvat kysymykset (LIITE 3). Puolistrukturoitua haastatteluosuutta seurasi myös vähän strukturoitu osuus, jossa haastateltava sai täydentää ja tarkentaa vastauksiaan ja näkemystään aihealueeseen liittyen. Haastattelujen löydöksiä ja tuloksia analysoitiin kappaleessa 7.1.3.

Haastattelukysymykset olivat kaikille samat. Haastattelun alussa käytiin läpi, että kysymykset, jotka eivät kohdistu omaan osaamisalueeseen voidaan ohittaa. Kysymykset teemoiteltiin kahteen luokkaan (TAULUKKO 5):

TAULUKKO 5: Haastattelukysymysten teemoittelu

1. Kyberturvallisuuden huomiointi organisaatioiden jatkuvuudenhallinnassa:
Kuinka hyvin kyberturvallisuus on otettu mielestänne otettu huomioon organisaatioiden jatkuvuudenhallinnassa nykyisin?
Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta? (Kyselyn avoin kysymys)
Jos organisaatio joutuu priorisoimaan toimenpiteitään suojatakseen jatkuvuuttaan, niin mitkä keinot näiden tulisi ensisijaisesti huomioida?
Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan? (Kyselyn avoin kysymys)
Miten vastaisitte tutkimuksen otsikon aiheeseen kysymysmuodossa: Miten näkisitte, että kyberturvallisuutta voitaisiin tehokkaimmin hyödyntää organisaatioiden jatkuvuudenhallinnassa nyt ja tulevaisuudessa?

2. Merkittävimmät kyberuhat ja nousevat teknologiat nyt ja tulevaisuudessa, sekä niiden vaikutukset organisaatioihin:
Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne. (Kyselyn avoin kysymys)
Mitkä ovat mielestänne merkittävimpiä nousevia teknologioita ja niiden aiheuttamia uhkia organisaatioiden jatkuvuuden kannalta nyt ja tulevaisuudessa?
Mitkä näette merkittävimmiksi uhkiksi ja mahdollisuuksiksi organisaatioiden kyberturvallisuuden ja jatkuvuudenhallinnan kannalta erikoistumisalaanne nähden?
Mitkä ovat kvanttiteknologian merkittävimmät uhkat ja mahdollisuudet organisaatioille nyt ja tulevaisuudessa?
Mitkä ovat 6G:n aiheuttamat merkittävimmät uhkat ja mahdollisuudet organisaatioille nyt ja tulevaisuudessa?
Näettekö nanoteknologian aiheuttavan uhkia nyt tai tulevaisuudessa? Jos, niin mitkä ovat merkittävimmät sen aiheuttamat uhkat?
Mitkä muut kehittyvät teknologiat ja trendit voivat uhata organisaatioiden jatkuvuudenhallintaa?

Tämän teemoittelun perusteella analysoitiin haastateltavien vastauksia, jotta saatiin asiantuntijanäkemystä empiirisen osion tueksi tutkimuskysymyksiin liittyen. Haastattelut tehtiin Jyväskylän yliopiston Teamsin kautta, jotta haastattelumateriaali saatiin tallennettua ja litteroitua. Tämä tehtiin haastateltavien suostumuksen jälkeen. Jokaiseen haastatteluun varattiin aikaa yksi (1) tunti. Käytännössä haastattelujen pituus vaihteli 30–60 minuutin välillä.

7 TUTKIMUSTULOKSET

Tutkimustuloksissa analysoitiin ensin erikseen tiedonkeräämismenetelmien avulla saadut tulokset, jonka jälkeen nämä koottiin lopussa yhteen kattavaa analyysia varten.

7.1 Aineiston analysointi

Aineiston käsittelyn ja analysoinnin lähtökohtana oli aineistolähtöinen, eli induktiivinen sisällönanalyysi, joka tarkoittaa analyysin perustamista suoraan aineistoon ilman ennakko-odotuksia, tai valmiita teorioita, edeten havainnoista yleisempiin väitteisiin (Saaranen-Kauppinen & Puusniekka, 2006). Aineistoa myös teemoiteltiin aihealueiden ja tutkimuskysymysten mukaan.

7.1.1 Kirjallisuuskatsaus

Kirjallisuuskatsaus antoi runsaan materiaalinsa puolesta hyvää kuvaa niin jatkuvuudenhallinnasta kuin kyberturvallisuudesta osa-alueina, sekä organisaatioita kohtaavista nykyisistä ja tulevista uhkista ja mahdollisuuksista kyber-fyysisessä maailmassa.

Organisaatioiden nykytilannetta koskeva materiaali jäi vähäisemmäksi, samoin tuore tutkimusaineisto, joten jo menetelmissä todetusti keskityttiin enemmän asiantuntijalähteisiin ja luotettavaksi todettujen toimijoiden luomaan materiaaliin.

Kirjallisuuskatsausta tehdessä nousi esiin, että selkeä jako jatkuvuudenhallinnan ja kyberturvallisuuden välillä ei ollut niin perusteltua, sillä monet kyberuhat voivat vaarantaa organisaation toimintojen jatkuvuuden, sekä samoin monet kyberturvallisuuden keinot suojaavat niitä, vaikka näitä ei olisi erikseen määritetty. Tutkimuskysymysten kannalta tämä kuitenkin ohjautui luontevasti merkittävimpien tunnistettavien uhkien ja toimintojen priorisointiin, vaikka selkeään erotteluun ei ollutkaan tarvetta. Näin ollen kirjallisuuskatsauksen analysoinnissa keskitytään merkittävimpien uhkien ja suojauskeinojen, sekä nykyisten ja tulevien trendien analysointiin katsoen, että ne voivat toteutuessaan kaikki uhata organisaatioin kriittisten toimintojen jatkuvuutta.

Kirjallisuuskatsauksen perusteella prosessit ja toimintatavat ovat usein huomattavan vaihtelevia riippuen muun muassa yritysten koosta, toimialasta, sekä käytettävissä olevista resursseista (esim. henkilöstö ja budjetti). Suuret ja reguloidut organisaatiot ja toimialat ovat korkeammalla, kun taas pienet ja reguloimattomat ovat usein matalammalla tasolla varautumisessaan. Tämä nostettiin esiin usein myös juuri toimittajaketjuriskeihin liittyen.

Yhteisistä tekijöistä voitiin nostaa merkittävimmiksi eri materiaalien kautta, miten suuri merkitys on sillä, että toiminta lähtee aina ylhäältä alaspäin ja sillä

tulee aina olla johdon tuki. Tämä tuli esiin oli sitten kyse kyberkypsyydestä, ennakoivasta varautumisesta, resursoinnista, tai kommunikoinnista. Kyberturvallisuuden johtaminen ei siis saa olla asiantuntijoiden yksinään suorittamaan toimintaa, vaan sillä tulee olla ylimmän johdon jatkuva tuki tilannetietoisuuden varmistamiseksi.

Riskienhallinta oli toinen merkittävä asia, joka tulee esiin riippumatta mitä materiaalia tutkittiin. Jos olisi tehty sanastoanalyysia eniten esiintyvistä termeistä riksienhallinta olisi ollut yleisimpiä. Tämän osalta myös peräänkuulutettiin läpi koko organisaation toimintojen tapahtuvaa ydintoimintaan sidottua riskienhallintaa, jossa ei eroteltu esim. kyberriskejä omaksi alueekseen, vaan ne olivat luonnollinen osa kokonaisriskienhallintaa.

Kolmas selkeä löydös oli, että monimutkaistuva kyber-fyysinen ja digitaalistuva maailma tarvitsee lakeja ja sääntöjä varmistaakseen turvallisuutta. Tämä voitiin todeta mm. Huoltovarmuuskeskuksen laajasta koosteraportista joka tehtiin toista kertaa. Enemmän reguloidut alat olivat paremmin varautuneita ja kypsyydeltään korkeammalla. Tässä tuli esille se, että ns. pakottavat toimet ohjaavat toimintaa paremmin, kuin pelkkä tilannetietoisuus ja uhkien tunnistaminen. Näyttäisi siltä, että monet organisaatiot eivät tee toimenpiteitä ellei heillä ole siihen jotain ulkoista herätettä, joka voi olla lakivaatimus, regulaatio, tai esim. alaan ja asiakkaisiin liittyvät standardivaatimukset (tietoturvan ja jatkuvuudenhallinnan standardit sekä viitekehykset). Organisaatioiden tulisi muistaa, että ne voivat käyttää standardeja ja kriteeristöjä ohjaamaan toimintaansa, vaikka tavoitteena ei olisikaan sertifiointi tai auditoinnin läpäiseminen, ja näin parantaa varautumistaan. Monet toimenpiteistä eivät vaadi suuria resursseja (esim. ihmisten kouluttaminen ja näiden osaamisen & tietoisuuden parantaminen. Ihmistekijä nousi kaikilla alueilla suurimmaksi riskiksi).

Nykyisiä merkittävimpiä uhkia tarkasteltiin tekemällä vertailu ENISAn, Crowdstriken ja Microsoftin raporttien välillä (TAULUKKO 6). ENISAn raportti ainoana vertailukohteina olleista antoi selkeän esiintyvyyden eri hyökkäyksille, joten sitä käytettiin vertailukohtana muihin raportteihin. Taulukon avulla voitiin nähdä, että kaikki toimijat nostivat samantyyppiset uhkat merkittävimmiksi. Vaikka erojakin oli, ne liittyivät enemmän painotuksiin ja sanamuotoihin, eivät niinkään erilaisiin uhkakenttiin.

Tummempi sininen taulukossa tarkoittaa, että raportin tiedot olivat yhteneväiset, vaaleampi sininen, että suoraa viittausta ei löytynyt sanamuodolta, mutta asia tuli esiin vertailukelpoisesti, ja valkoinen, että mainintaa ei löytynyt. Näin nollapäivähaavoittuvuudet nousivat esiin vain ENISAn raportissa, mutta koska muissa raporteissa puhuttiin haavoittuvuuksista yleisesti ei voida sulkea pois, etteikö nollapäivähaavoittuvuuksia olisi sisällytetty näihin. Näin ollen taulukon avulla voitiin poimia organisaatioihin kohdistuvat tämänhetkiset merkittävimmät kyberuhat melko luotettavasti kyberturvallisuuden keinojen priorisoimisen tueksi.

TAULUKKO 6: Raporttien uhkien vertailu

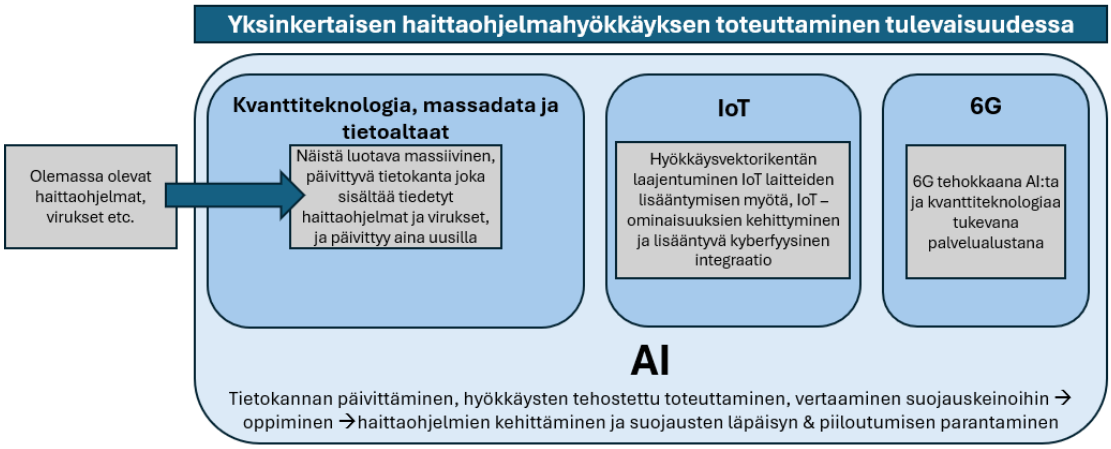
ENISA raportti 2024	Crowdstrike raportti 2024	Microsoft raportti 2024
Palvelunestohyökkäykset DoS / DDoS	Palvelunestohyökkäykset DoS / DDoS	Palvelunestohyökkäykset DoS / DDoS
Kiristysohjelmahyökkäykset	Kiristysohjelmahyökkäykset	Kiristysohjelmahyökkäykset
Dataan kohdistuvat hyökkäykset	Osana muita uhkia raportin perusteella	Osana muita uhkia raportin perusteella
Sosiaalinen manipulointi / tietojen kalastelu	Sosiaalinen manipulointi / tietojen kalastelu	Sosiaalinen manipulointi, tietojen kalastelu ja petokset
Haittaohjelmat	Haittaohjelmat	Haittaohjelmat
Toimitusketjuhyökkäykset	Toimitusketjuihin kohdistuvat uhat	Toimitusketjuihin kohdistuvat uhat osana OT -uhkia
Valtiollisen tason kyberuhkat	Valtiollisen tason kyberuhkat (vaalivaikuttaminen)	Valtiollisen tason kyberuhkat ja hybridisodankäynti
Nollapäivähaavoittuvuudet	Ei mainittu erikseen, haavoittuvuudet mainittu yleisesti	Ei mainittu erikseen, haavoittuvuudet mainittu yleisesti
Pilvipalveluihin kohdistuvat hyökkäykset	Pilvialustoihin ja -toimintoihin kohdistuvat uhat	Pilvipalveluihin kohdistuvat hyökkäykset
Käyttäjäoikeuksiin kohdistuvat hyökkäykset	Käyttäjäoikeuksiin kohdistuvat hyökkäykset	Käyttäjäoikeuksiin kohdistuvat hyökkäykset
Hallinnoimattomat laitteet ja alustat ja tuotantojärjestelmien teknologiaan (OT) kohdistuvat hyökkäykset varsinkin kriittiseen infrastruktuuriin kohdistuen	Hallinnoimattomat laitteet ja alustat ja tuotantojärjestelmien teknologiaan (OT) kohdistuvat hyökkäykset varsinkin kriittiseen infrastruktuuriin kohdistuen	Hallinnoimattomat laitteet ja alustat ja tuotantojärjestelmien teknologiaan (OT) kohdistuvat hyökkäykset varsinkin kriittiseen infrastruktuuriin kohdistuen
LOTS ja LOTL, piiloutuminen järjestelmiin ja lateraalinen liikkuminen järjestelmien sisällä	Piiloutuminen järjestelmiin ja lateraalinen liikkuminen järjestelmien sisällä	Piiloutuminen järjestelmiin ja lateraalinen liikkuminen järjestelmien sisällä
Tekoäly osana hyökkäyksiä	Tekoäly osana hyökkäyksiä	Tekoäly osana hyökkäyksiä

Merkittävimpien uhkien tunnistamisen jälkeen harkittiin tehdä kartoitus suojaustoimenpiteistä kirjallisuuskatsauksessa tunnistettuja keinoja apuna käyttäen. Tästä kuitenkin luovuttiin, sillä katsottiin, että se ei tuo tutkimukseen sellaista lisäarvoa mitä ei olisi jo paremmin avattu tutkimuksen lähdemateriaaleissa. Tärkeintä oli tehdä vertaileva kartoitus priorisoitavista uhista, jotta organisaatiot voivat kohdistaa suojauskeinonsa tehokkaimmin.

Yleisesti voitiin kuitenkin tunnistaa, että teknisten suojauskeinojen ei tulisi olla ensisijainen lähestymistapa kyberturvallisuuteen, vaikka ne ovatkin kriittinen osa kokonaisuuden lopputuloksena. Ensisijaisesti organisaatioiden tulisi keskittyä huomioimaan kyberturvallisuus osana (liike)toimintaansa ja jatkuvuudenhallintaa siten, että osa-alue ei ole erillinen, vaan se on integroitu osaksi johdon strategiaa, sitoutumista ja riskienhallintaa. Tätä kautta organisaatiolle syntyy kuva niin kriittisistä suojattavista toiminnoistaan, kuin niihin vaikuttavista uhkista, niiden suojaamisen resurssoinnista, sekä tehokkaimpien suojausmenetelmien priorisoinnista. Kun tähän kokonaisuuteen yhdistetään henkilöstön osaamisen parannus ja ylläpito (koulutukset), sekä toimintojen ja prosessien testaaminen, niin kokonaisuus on hallittu ja resilientimpi. Tämä lähestymistapa tuli esiin läpi materiaalien, ja painotti

standardien ja viitekehysten mallia lähestyä kyberturvallisuutta osana jatkuvuudenhallintaa.

Tulevaisuuden merkittävimmät kyberuhat ja kyberturvallisuuden mahdollisuudet kiteytyivät paljolti teköälyn ympärille. Tällä ei tarkoiteta, että tekoäly olisi tutkimusmateriaalien perusteella noussut ainoana uhkana esiin, vaan, että sen avulla pystytään tehostamaan, kehittämään ja muovaamaan niin hyökkäys- kuin suojausmenetelmiä siinä määrin, että tällä hetkellä ei pystytä vielä hahmottamaan uhkakentän kokonaiskuvaa. Tästä voitiin johtaa mm. seuraava esimerkki (KUVIO 11) nousevia teknologioita hyödyntäen siitä, miten haittaohjelmat voivat toimia tulevaisuudessa vaatien hyökkääjältä joko tilauksen verkosta (kyberrikolliset), tai minimaalisen määrän osaamista:



KUVIO 11: Esimerkki haittaohjelmahyökkäyksestä tulevaisuudessa

Kyseinen hyökkäysmalli on vasta tulevaisuutta, ja arviot vaihtelivat 5-10 vuoden välillä milloin tämä voisi olla mahdollista. Kilpajuoksu on siis käynnissä hyökkäävien tahojen, ja puolustustoimenpiteiden välillä, mutta kokonaisvaikutukset mitä hybridiuhat voisivat olla ja aiheuttaa vaativat enemmän tutkimusta.

Kirjallisuuskatsauksella ei saatu tuotettua juurikaan uutta tietoa, vaan enemmän tehtyä vertailua eri asiantuntijaorganisaatioiden välillä uhkakuvista ja kyberturvallisuuden priorisoitavista hallintakeinoista, sekä kerättyä tietoa merkittävimmistä nykyisistä ja tulevista trendeistä kybermaailmaan liittyen. Näitä käytettiin vertailussa empiirisen tutkimuksen osuuteen. Kirjallisuuskatsaus jätti avoimeksi myös kysymykset, miten organisaatiokenttä yleensä (pois lukien huoltovarmuuskriittiset organisaatiot) kokee oman varautumisensa tilanteen, miten nämä ovat huomioineet kyberturvallisuuden osana jatkuvuudenhallinnan menettelyjään, sekä miten kyberturvallisuudella voidaan tehostaa jatkuvuudenhallintaa, sekä näiden keskinäistä arvoa toiselleen parantaa. Näihin perehdyttiin paremmin kyselyssä ja haastatteluissa.

7.1.2 Kyselyt

Kyselyn päätavoite oli saada tietoa organisaatioiden varautumisesta ja koetuista kyvykkyyksistä vastattaessa tutkimuskysymyksiin. Tämän vuoksi kysely keskittyi tutkimuksen alakysymyksiin b. ja c. Alakysymyksiä a. ja d. käsiteltiin kattavammin kirjallisuuskatsauksen, sekä haastatteluiden avulla.

Kyselyyn vastasi 27 henkilöä. Vastaukset jakautuivat:

- Pienet ja keskisuuret organisaatiot: 37% / 10 vastaajaa,
- Suuret tai kriittiseen infrastruktuuriin kuuluvat organisaatiot 44% / 12 vastaajaa,
- Organisaatiot yleisesti 18,5% / 5 vastaajaa.

Tuloksia vertailtiin laskemalla sekä vastaajittain, että kysymysten osalta prosenttituloksista keskiarvo, mediaani ja moodi. Täten voitiin nähdä niin vastaajien näkemys kysymyksen tilanteesta organisaatioissa, kuin mikä oli trendi kaikkien vastaajien keskuudessa yksittäisen kysymyksen osalta. Laskentatoimitukset tehtiin siis sekä kysymyksittäin, jotta pystyttiin ymmärtämään miten eri, asiat on huomioitu organisaatioissa kokonaisuutena, että vastaajittain jotta saatiin myös organisaatiotyyppien välisiä eroja selvitettyä. Alla olevassa taulukossa (TAULUKKO 7) on yhdistetty nämä tulokset visuaaliseen muotoon. Oikealta kolumneista löytyvät vastaajien arvot: Keskiarvo (ka), mediaani (Md) ja moodi (Mo). Kysymysten arvot löytyvät alhaalta samalla tavalla jaoteltuna. Vastaukset myös jaoteltiin organisaatiotyypeittäin, sekä kysymysten osioiden mukaisesti (osio 1, osio 2, osio 3) teemoitellen. Vaakariveiltä löytyvät yksittäisten vastaajien vastaukset kysymyksittäin, jotka on numeroitu kolumneissa 1.-19. Avoimet kysymykset 20.-23. jätettiin tästä pois koska niillä ei ole arvoja. Oikeasta laidasta löytyvät yksittäisen vastaajan arvot kaikkiin kysymyksiin. Pystykolumnien avulla voitiin laskea arvot kysymyksittäin kaikkien vastaajien keskuudessa, ja niiden arvot löytyvät taulukon alaosasta.

TAULUKKO 7: Kyselyn tilastollinen analysointi

		Kysymykset																			Vastaajan arvot:		
		Osio 1						Osio 2						Osio 3									
Organisaatio-tyypit		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	ka	Md	Mo
Pienet ja keskisuuret organisaatiot	1	3	3	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	1	2,1	2	2
	1	5	4	4	3	3	3	4	4	4	3	3	4	3	4	4	3	4	3	2	3,5	4	4
	1	4	4	4	3	3	3	4	3	4	3	3	4	4	4	2	3	3	3	3	3,4	3	3
	1	5	4	4	2	4	2	3	2	5	5	2	2	4	5	4	4	5	3	1	3,5	4	4
	1	4	4	4	3	3	4	4	3	4	3	4	4	4	4	4	4	4	4	2	3,7	4	4
	1	4	5	4	3	3	3	4	4	4	3	4	4	3	3	3	3	3	3	3	3,5	3	3
	1	5	4	3	3	2	3	4	3	3	2	3	3	4	3	3	4	3	4	3	3,3	3	3
	1	3	4	3	2	2	2	2	2	4	2	2	3	2	4	2	2	2	3	2	2,5	2	2
	1	4	4	5	3	3	4	4	3	2	2	3	4	2	3	5	5	3	5	2	3,5	3	3
	1	3	3	2	2	2	1	2	2	2	1	2	1	2	2	2	1	3	4	1	2	2	2
Suuret ja kriittiseen infrastruktuuriin kuuluvat organisaatiot	2	3	3	3	2	3	3	3	4	3	3	3	3	3	4	2	3	3	4	2	3	3	3
	2	4	4	3	3	3	3	4	3	3	4	4	3	3	4	2	2	3	3	2	3,2	3	3
	2	3	3	3	2	1	1	2	2	3	2	2	2	2	2	1	2	2	2	2	2,1	2	2
	2	5	5	5	4	4	4	4	4	5	2	2	4	4	4	2	4	4	2	2	3,7	4	4
	2	5	5	5	4	4	5	4	5	5	4	5	5	4	4	5	5	5	5	4	4,6	5	5
	2	3	4	3	2	2	2	2	2	2	2	2	2	3	3	4	4	2	3	2	2,6	2	2
	2	5	4	3	3	3	4	3	2	3	2	3	4	3	3	2	4	2	4	3	3,2	3	3
	2	3	3	4	4	2	3	4	2	4	2	2	3	4	4	4	4	4	4	2	3,3	4	4
	2	4	4	3	2		3	3	2	2		3	3	3	3			3	3		2,9	3	3
	2	4	4	5	3	3	3	4	4	4	3	3	3	4	3	2	2	4	3	2	3,3	3	3
	2	4	4	5	3	3	3	4	4	3	3	4	4	4	4	4	4	2	2		3,6	4	4
	2	3	3	4	2	3	3	2	4	3	2	3	4	3	2	1	2	2	3	2	2,7	3	3
Organisaatiot yleisesti	3	5	5	5	4	3	3	4	4	4	3	3	5	4	4	5	4	4	4	3	4	4	4
	3	3	3	3	2	2	3	2	2	3	3	2	2	3	3	2	2	1	2	2	2,4	2	2
	3	3	3	3	2	2	2	3	2	2	2	2	2	1	1	1	2	2	1	1	1,9	2	2
	3	3	3	3	2	1	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2,2	2	2
	3	3	3	3	2	2	3	2	2	2	2	3	3	3	3	2	4	2	2	2	2,5	2	2
Kysymyksen arvot:																							
keskiarvo (ka)		3,8	3,8	3,6	2,7	2,6	2,9	3,2	2,9	3,2	2,6	2,8	3,1	3,1	3,2	2,8	3,1	2,9	3,1	2,1			
mediaani (Md)		4	4	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	2			
moodi (Mo)		3	4	3	2	3	3	4	2	2	2	2	4	3	4	2	4	2	3	2			

Taulukkoon luokiteltiin vastaukset väreittäin numero yhden (1) tarkoittaessa taulukon 2 mukaisesti joko ”erittäin huonosti” tai ”täysin eri mieltä”, kun taas numero viisi (5) tarkoitti ”Erittäin hyvin” tai ”Täysin samaa mieltä”. Taulukosta poistettiin arvo, jos henkilö ohitti kysymyksen (harmaa).

Tämän jälkeen tehtiin tilastollinen analyysi organisaatiotyypeittäin teemoittelun mukaan laskemalla näiden kaikkien vastausten arvoista organisaatiotyypin keskiarvo, mediaani ja moodi, jotta saatiin näiden tilanne kokonaisuutena paremmin esiin (TAULUKKO 8).

TAULUKKO 8: Tilastollinen analyysi organisaatiotyypeittäin

Organisaatiotyyppi	**Vastaukset**	**Arvot**		
	lukumäärä	keskiarvo	mediaani	moodi
Pienet ja keskisuuret organisaatiot	190	3,1	3	3
Suuret ja kriittiseen infrastruktuuriin kuuluvat organisaatiot	222*)	3,2	3	3
Organisaatiot yleisesti	95	2,6	2	2
*) = "ohita kysymys/ohita väittämä" poistettu arvoista				

Taulukosta saadut tulokset olivat sinällään mielenkiintoisia, että pienten ja keskisuurien organisaatioiden koettujen kyvykkyyksien ja varautumisen, sekä suurten ja kriittiseen infrastruktuuriin kuuluvien yritysten välinen ero oli hyvin pieni, eli vastaajat kokivat molempien varautumisasteen ja kyvykkyydet samankaltaiseksi (keskiarvo 3,1 ja 3,2). Mutta, vastaajat, jotka vastasivat organisaatioiden osalta yleisesti, kokivat tilanteen negatiivisempana keskiarvon jäädessä 2,6:een. Kyselyvastausten perusteella ei voitu päätellä miksi näin oli, mutta ero voi liittyä vastaajien oletuksiin organisaatiokentältä yleisesti, kun taas henkilöt, jotka valitsivat tietyn organisaatiotyypin, omasivat käsityksen tyypin sisältä. Vastausmäärä oli kuitenkin niin pieni, että tämän osalta ei voitu tehdä syväluotaavaa eroa organisaatiokentittäin, mutta saatiin kokonaisarvio yhteisesti organisaatioista tarkasteltavaksi, ja suurempana arvona saatiin vastaajien näkemykset osioittain ja kysymyksittäin, joiden perusteella arviota tilanteesta pystyttiin tekemään paremmin. Kyselyn tulos oli myös ristiriidassa kirjallisuuskatsauksen tulosten kanssa, jossa suurien ja kriittiseen infrastruktuuriin kuuluvien organisaatioiden nähtiin olevan korkeammalla kypsyysasteella.

Seuraavaksi laskettiin arvot kyselyn eri osioiden teemoittelun mukaisesti (TAULUKKO 9), jotta saatiin vielä tietoa oliko valmistautumisen ja suunnittelun (Osio 1), koettujen valmiuksien (Osio 2), sekä metodien, prosessien ja työkalujen (Osio 3) osalta selkeitä eroja.

TAULUKKO 9: Tilastollinen analyysi vastausosioittain

Osio	**Vastausten määrä**	**Arvot**		
	lukumäärä	**ka**	**Md**	**Mo**
Osio 1: Organisaatioiden jatkuvuudenhallintaan liittyvä **valmistautuminen ja suunnittelu** keskittyen kyberturvallisuuteen yleisesti.	161*)	3,2	3	3
Osio 2: Organisaatioiden **koettu valmius** vastata vakaviin jatkuvuuteen vaikuttaviin kyberuhkiin, -poikkeamiin ja -hyökkäyksiin.	161*)	3	3	2
Osio 3: Organisaatioiden kyberturvallisuuteen kohdistetut **metodit, prosessit ja työkalut**.	185*)	2,9	3	2
*) = "ohita kysymys/ohita väittämä" poistettu arvoista				

Tämän taulukon perusteella voitiin nähdä tulosten olevan melko keskivertoja, mutta valmistautumisen ja suunnittelun (keskiarvo 3,2, moodi 3) nähtiin olevan kuitenkin paremmalla tasolla, kuin koettujen valmiuksien ja itse tekemisen metodien, prosessien ja työkalujen (keskiarvot 3 ja 2,9, ja moodit 2 molemmissa). Tämä antoi alustavaa indikaatiota siitä, että organisaatioiden teoreettinen valmistautuminen on paremmalla tasolla, kuin itse suorittaminen ja toiminnot asioiden eteen.

Tämän jälkeen tarkasteltiin selkeimpiä kyselystä esiin nousseita trendejä, joiden arvot antoivat kysymyksittäin indikaatiota tilanteesta. Kysely käsitteli organisaatioiden kyberturvallisuutta ja jatkuvuudenhallintaa osioissa määritetyistä kulmista kokonaisuutena. Yksittäiset kysymykset käsittelivät kuitenkin tarkemmin organisaatioiden riskienhallintaa, resursseja, toimittaja- ja alihankintaketjujen hallintaa, harjoittelua ja testaamista sekä nykyisen ja tulevan vertailua.

Tässä tarkastelussa vastausten perusteella suurimmiksi haasteiksi koettiin:

- Kaikkein merkittävimmäksi puutteeksi nähtiin toimittajien ja alihankkijoiden kouluttaminen organisaatioiden kyberturvallisuuteen ja jatkuvuudenhallintaan liittyen (kysymys 19., ka 2,1).
- Alihankintaketjujen hallinta kokonaisuudessaan ja niihin liittyvien riskien tunnistaminen. (kysymykset 5., ka 2,6 ja 10., 2,6).
- Kyberturvallisuuteen varattujen resurssien riittävyys (kysymys 4., ka 2,7).
- Harjoitus- ja testaustoiminnan riittävyys (kysymys 15., ka 2,8).
- Nouseviin uhkiin vastaamisen valmiudet (kysymykset 6, ka 2,9 ja 11., ka 2,8).
- Merkittävistä hyökkäyksistä palautuminen (kysymys 8., ka 2,9).
- Kriisi- ja poikkeustilanneviestinnän riittävyys (kysymys 17., ka 2,9).

Kaikissa yllä olevissa keskiarvo jäi alle 3, Tämän lisäksi kysymysten 10. (hankintaketjujen kautta tapahtuvat hyökkäykset), 15. (organisaatioiden riittävä harjoittelu ja testaus) ja 19. (toimittajien ja alihankkijoiden kouluttaminen) sekä mediaani ja moodi olivat molemmat arvolla 2.

Parhaimmiksi organisaatioissa arveltiin kyvykkyydet (ka yli 3,5) liittyen:

- Suojattavien toimintojen, omaisuuden ja resurssien tunnistamiseen (kysymys 1., ka 3,8).
- Kyberturvallisuuden huomiointiin osana jatkuvuudenhallintaa (kysymys 2., ka 3,8).
- Kyberturvallisuusriskien tunnistamiseen (kysymys 3., ka 3,6).

Havaituista vahvuuksista ainoastaan kysymys 2. (kyberturvallisuuden huomiointi osana jatkuvuudenhallintaa) sai sekä mediaan että moodin arvoksi 4.

Löydösten perusteella voitiin vetää johtopäätöksiä organisaatioiden arvioiduista kyvykkyyksistä kyselyn suppeuden takia melko rajallisesti, ja tuloksia tarkastellaan myöhemmin analyysien yhteenvedossa. Mutta, selkein löydös oli, että valmistautumisen ja tunnistamisen koettiin olevan pääosin melko hyvällä tasolla, mutta hajontaa ja heikkouksia ilmeni enemmän, kun käsiteltiin operatiivista toimintaa aihealueeseen liittyen. Toimittajahallinnan koettiin läpi löydösten olevan heikoin osa-alue, ja myös riittävä harjoittelu ja testaus jakoivat eniten mielipiteitä ja koettiin haasteeksi.

Avoimet kysymysten osalta harkittiin pitkään, miten tulokset olisi järkevintä esittää jotta niistä saataisiin mittavin hyöty. Vastaukset avoimiin

kysymyksiin päätettiin liittää raakadatana osaksi liitteitä (LIITE 4), ja tähän osioon stilisoitiin näistä esiin nostetut huomiot taulukoihin kysymyksittäin ja tehtiin jokaisesta lyhyt yhteenveto (TAULUKOT 10, 11, 12 ja 13).

Kysymys 21: *"Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta?"*

TAULUKKO 10: Kysymys 21. vastaukset ja esiintyvyys vastauksissa

Vastaukset	**esiintyvyys**
Ohjeistusten käyttöön implementointi	1
Koulutus organisaatioista riippumatta	1
Harjoitukset sisältäen käytännön harjoittelun	1
Johdon roolin ja vastuiden merkitys	2
Organisaatioiden tekninen kyvykkyys	1
Alihankintaketjujen kyvykkyydet ja vastuut sisältäen riskienhallinnan	3
Riittävä resurssointi (investointi, talous, ajankäyttö)	5
Sopimustekniset järjestelyt jatkuvuudenhallinnan kybernäkökulmaan liittyen	1
Tieto- ja kyberturvallisuuskoulutusten kehittäminen (miksi tärkeää, oman toiminnan vaikutus, uhkakentät jne.)	1
Jatkuvuussuunnitelmat ja toipumissuunnitelmat kuntoon	1
Dokumenttien ajantasaisuus	1
Riskienhallinta	1
Suojattavien kohteiden tunnistaminen (assets)	3
P-k -organisaatioiden ymmärrys kyberuhkien vaikutuksesta omaan toimintaan, varsinkin ei IT -keskeisillä aloilla	1
ohjelmien (software) ja laitteiden (hardware) päivitykset (haavoittuvuuksilta suojautuminen)	1
Laitteiden fyysinen suojaus ja hallinta (mm. vesivahingot)	1
Varmentamisen suojaaminen ja palautumisen testaaminen.	1
Riippuvuuksien tunnistaminen (sisäiset ja ulkoiset)	2
Toimenpiteiden priorisointi	2
Vakuuttaminen	1

Tulee huomioida, että vastausten esiintyvyyden arviointi on subjektiivinen, mutta analysoinnissa pyrittiin ottamaan vastaus osaksi jo aiemmin esiintynyttä vain, jos ne jakoivat yhteisen sanan, tai selkeästi saman tarkoituksen. Eniten esiin nousivat resurssointiin panostamisen tärkeys, alihankintaketjujen turvallisuuden huomiointi, sekä suojattavien kohteiden tunnistaminen. Tähän osioon otettiin myös kaksi suojautumiseen liittyvää vastausta kysymyksen 21 puolelta.

Kysymys 22: *" Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne."*

TAULUKKO 11: Kysymys 22. vastaukset ja esiintyvyys vastauksissa

Vastaukset	esiintyvyys
Alihankinta- ja toimitusketjut (turvallisuus, jatkuvuus,)	4
Avoimen lähdekoodin sovellukset ja modulit	1
Haavoittuvuudet (sisältäen nollapäivähaavoittuvuudet)	1
ihminen (käyttäjät)	3
Pilvipalveluiden ongelmat (esim. Azure, Crowdstrike, Cloudfare)	1
Tietojen kalastelu ja social engineering	3
Tietovuodot ja -murrot	5
Valtiollisen tason hyökkäykset	2
Uudet teknologiat ja niiden kautta hyökkäyspinta-alan laajentuminen (käyttöönotto, rikolliset)	1
Reagointiajan lyhentyminen hyäkkäyksiin vastattaessa	1
Riskienhallinnan puutteet (mm. että riskejä ei arvioida kokonaisuutena kyberturvallisuuden näkökulmasta)	1
Disinformaatio	2
Identiteettivarkaudet	1
Vanhat järjestelmät jotka eivät tue tietoturvatarpeita ja vanhentuva tekniikka yleisesti	2
Kiristyshaittaohjelmat	2
Palvelunestohyökkäykset	2
Tietojen tuhoaminen	1
Tiedoilla kiristäminen (ei haittaohjelma kautta tapahtuva)	1
AI / tekoäly	3
Venäjä	1
3. maailmansota / sotakonfliktien laajeneminen globaalimmiksi	1
Resurssit ja niiden polarisoituminen organisaatioissa	2
Osaaminen (esim. uusien teknologioiden vaatimukset ja monimutkaistuvat ympäristöt)	1

Vastauksissa eniten esiin nousivat tietovuotoihin ja -murtoihin sekä toimittajaketjuihin kohdistuvat uhat. Myös tietojen kalastelu, ihmiset riskitekijänä ja tekoäly nousivat useimmin esiin vastauksissa. Tietovuotojen osalta on huomioitava, että ne voivat olla lopputulos monista yllä mainituista uhkista, vaikka niitä ei erikseen mainittu.

Kysymys 23: *”Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan?”*

TAULUKKO 12: Kysymys 23. vastaukset ja esiintyvyys vastauksissa

Vastaukset	esiintyvyys
Tekoälyn hyödyntäminen	2
Palomuurit (sisältäen WAF)	3
SIEM / SOAR	2
Anomalioiden tunnistukseen kykenevät järjestelmät	1
XDR	1
SSO (Single sign-on)	1
Varmuuskopiot	1
CSOC/SOC -palvelu (sisäinen tai ulkoinen), tai havainnointipalvelut / valvotut järjestelmät	4
Turvallinen järjestelmä-/verkkoarkkitehtuurisuunnittelu	1
Turvallinen ohjelmistosuunnittelu ja elinkaarihallinta	1
Määrämuotoinen hallinnollinen malli / viitekehysten käyttö	1
Päivityssyklit	1
Toimitusketjujen turvallisuus	1
Koulutukset ja osaamisen varmistaminen sisältäen käyttäjäkoulutukset (riittävän usein, kattavuus) sisältäen johdon osaamisen ja toiminnan	6
Riittävä resurssointi sisältäen riittävät investoinnit	2
Riittävät ratkaisut organisaatioiden tarpeisiin	2
Nollatietokoneet	1
Päivitetyt reitittimet ja keskittimet	1
Salasanapolitiikka	1
Riittävä dokumentaatio	1
Harjoittelu (uhkatilanteet, palautuminen, osallistujien kattavuus)	3
Testaukset (haavaskannerit, penetraatiotestaukset	2
Testaustulosten hyödyntäminen kehitystyössä ja korjauksissa	1
Tehokas ja kattava riskienhallinta, joka kattaa myös johdon	1
Jatkuvuussuunnittelu (sisältäen toimivat ja käyttökelpoiset liiketoiminnan vaikutusanalyysit (BIA) (myös tietotekniseen infraan ja tietojärjestelmiin), riippuvuuksien tunnistamisen ja suojattavan omaisuuden tunnistamisen	2
Vikasietoisuuden varmistaminen	1
Kybersuojausten kehittäminen	1

Suojautumisen työkaluissa nousi kaikkein merkittävimpänä esiin ihmistekijä, sekä siihen liittyen kouluttaminen ja harjoittelu mikä alleviivaa asian merkittävyyttä, sillä riippumatta vastaustavasta tämä oli tunnistettu vastaajien keskuudessa tärkeäksi suojautumiskeinoksi. Vasta tämän jälkeen tuli SOC/CSOC tai vastaava palvelu, sekä palomuurit teknisenä ratkaisuna.

Viimeisenä osiona (kysymys 24.) oli ”Vapaa sana” johon vastaajat saattoivat lisätä omia lisähuomioitaan aihealueeseen ja tutkimusaiheeseen liittyen. Nämä stilisoitiin alla olevaan taulukkoon (TAULUKKO 13).

TAULUKKO 13: Kyselyn Vapaa sana

Vastaukset
Regulaatioiden ja lainsäädännön merkitys ohjaajina ja varmistajina on yhä merkityksellisemmässä roolissa
Kriittinen infrastruktuuri suhteellisen hyvin varautunut, mutta polarisaatiota on eri sektoreiden sisällä ja välillä --> keskiarvo ei riitä, vaan huonosti varautuneiden tasoa pitää pystyä nostamaan
Johtamisella on hyvin merkittävä rooli (sitoutuminen, vastuut)
Viestinnän merkitys niin kriisi- kuin normaalitilanteissa (rauhoittelu, oikea-aikaisuus, varmuus, ohjeet jne.) tulee olla osana jatkuvuudenhallintaa, mutta korostuu kyberpoikkeamissa biaksen ollessa Venäjän toiminnassa, vaikka vastuussa olisivat muut tahot (rikolliset, haktivistit jne.)
"Toivottavasti ehditään tekemään ennen kuin jotain sattuu" -ajatus
Kyberturvan ja hyökkäystekniikkojen ymmärtäminen auttaa
Penetraatiotestejä suorittavia yrityksiä tarvitaan lisää, jotta eri tason toimijat voivat paremmin valita itselleen sopivan.
Tiedon jakaminen ja ymmärtämisen lisääminen organisaatioissa joka tasolla kyberturvallisuuteen ja jatkuvuudenhallintaan liittyen
Oman vapaa-ajan toiminnan mahdollinen vaikutus työnantajaan.
Kyberuhat liian usein "IT asia" eikä nähdä kyber-fyysistä maailmaa ja kokonaisuutta
Lisätutkimusaihe: "*Paljonko oikeasti resursseja eri kokoiset organisaatiot käyttävät tieto- ja kyberturvallisuuden varmistamiseen. Samalla olisi hyvä tutkia, että miten käytetyt resurssit korreloivat poikkeamien määrään. Meillä on jonkun verran subjektiivisia kyselytutkimuksia (kuten tässäkin kyselyssä), mutta tiedossa ei ole, että Suomessa olisi tehty tutkimusta, jossa olisi kysytty absoluuttisia määriä. Australiassa ACSC on tehnyt esim vastaavan selvityksen paikallisten PK-yritysten resursseista*"
Toivottu kyselyn alkuun kyberturvallisuuden määritelmää, koska termin merkitys voi vaihdella vastaajittain.

Vapaassa sanassa nostettiin esiin huomionarvoisia asioita, jotka nousivat osittain esiin aiemmissa avoimissa kysymyksissä, mutta tämän lisäksi nostettiin esiin tärkeänä tekijänä kehittyvän regulaation ja lainsäädännön merkitys toiminnanohjaajana. Lisäksi huomionarvoista oli kommentti siitä, että ns. keskiarvoajattelu ei ole hyvä, vaan tulee huomioida heikoin lenkki, ja pyrkiä nostamaan heikoimpien toimijoiden tasoa. Myös oman vapaa-ajan toimien vaikutuksen ymmärtäminen oli hyvä nosto, samoin huomio siitä, että kyberturvallisuus olisi ollut hyvä määritellä kyselyn alussa. Tämän osalta tutkija harkitsi asiaa kyselyä tehdessään, mutta koska kysely oli suunnattu asiantuntijoille, ja termille on kuitenkin melko vakiintunut käsitys, jätettiin tämä tekemättä. Huomio oli silti validi, mutta aineiston analyysin perusteella ei noussut selkeää indikaatiota, että vastaajat eivät olisi ymmärtäneet aihealuetta. Viimeisenä nostettavana huomiona saatiin ehdotus tutkimusaiheesta liittyen siihen, paljonko resursseja organisaatioissa käytetään, ja miten käytetyt resurssit korreloivat poikkeamien määrään.

Kaikkiaan kyselyn vastauksissa nousi kaikkein vahvimmin esiin ihmistekijän merkitys ja osaamiseen liittyvät tekijät (koulutukset, harjoitukset, osaaminen), joka on linjassa mm. kirjallisuuskatsauksen tulosten kanssa.

7.1.3 Haastattelut

Haastatteluilla haluttiin saada syvempää laadullista ymmärrystä aihealueeseen, sekä tietoa tutkimuskysymyksiin liittyen kirjallisuuskatsauksen ja kyselyn tueksi. Kaikkien haastateltavien kanssa käytettiin samaa haastattelupohjaa (LIITE 3), joten myös haastatteluja arvioitiin yhdessä kysymyksittäin ja teemoittelun mukaan, eikä jokaista haastateltavaa käsitelty erikseen.

Haastateltavina oli neljä asiantuntijaa, joilla oli kohdistettua tai laaja-alaisempaa osaamista tutkimusaiheeseen nähden. Haastateltavat eivät osallistuneet

tutkimukseen organisaatioidensa edustajina, vaan yleisesti kyberturvallisuuden ja/tai jatkuvuudenhallinnan asiantuntijoina. Heidän vastauksensa haastattelukysymyksiin eivät liity työnantajaorganisaatioihin millään tavalla, vaan annettiin yleisluontoisesti aihealuetta tarkastellen.

Haastatteluihin osallistuivat Jouni Flyktman (Valtiollinen kyberturvallisuus, kyberpuolustus, kvanttiteknologia), Kirsi Karlamaa (Radio- ja avaruustekniikka, verkkoteknologiat, kyberturvallisuus ja huoltovarmuus), Kimmo Rousku (Kyberturvallisuus, riskienhallinta, jatkuvuudenhallinta, digiosaamisen kehittäminen) ja Suvi Lampila (tekninen tietoturva, kvanttiturvallinen salaus, sertifikaatti- ja verkkoprotokollat). Haastatelluille esitetyt kysymykset löytyvät liitteestä 3 ja ne teemoiteltiin kyberturvallisuuden huomiointiin organisaatioiden jatkuvuudenhallinnassa, sekä merkittävimpiin organisaatioihin vaikuttaviin kyberuhkiin ja nouseviin teknologioihin nyt ja tulevaisuudessa.

Haastattelun ensimmäisenä aiheena oli asiantuntijoiden näkemys siitä kuinka hyvin kyberturvallisuus on huomioitu organisaatioiden jatkuvuudenhallinnassa tällä hetkellä. Vastaukset tähän vaihtelivat jonkin verran, mutta yhtenevä kanta oli, että eroa organisaatioiden välillä on selkeästi olemassa, ja turvallisuuskriittiset sekä reguloidut organisaatiot ovat varautumisessaan paremmalla tasolla, kun taas muulla puolella on enemmän hajontaa. Kirsi Karlamaa viittasi Huoltovarmuuskeskuksen Kyberkypsyyden selvitysraporttiin (HVK, 2022), joka antoi myös selkeän indikaation siitä, miten sääntely ohjaa organisaatioiden varautumista ”*Mitä pidempään alaa on säännelty, joka on pakottanut ne yritykset säännösten mukaisesti varautumaan ja huolehtimaan tietoturvallisuudestaan, sen paremmalla tolalla ne ovat mikä on suora indikaatio siihen, että sääntelyllä on väliä. NIS2 tulee entisestään parantamaan sitä.*”. Haastattelut vahvistivat muun tutkimusmateriaalin tulosta siitä, että pakottava ja ohjaava lainsäädäntö, standardit, ja regulointi ovat vahvimmin ohjaavia tekijöitä varautumisessa.

Aihealueeseen mitä organisaatioiden tulisi ottaa huomioon kyberturvallisuuden osalta jatkuvuudenhallinnassaan, ja mitä näiden tulisi priorisoida näkyivät selkeämmin haastateltavien taustat ja erikoisosaaminen. Silti päällimmäisinä asioina nousivat esiin johdonmukaisesti kriittisten toimintojen tunnistamisen merkitys sekä niiden suojaamisen priorisointi, johdon rooli kokonaisuudessaan, sekä riskinhallintalähtöinen ja ennakoiva toiminta kaiken perustana. Lisäksi toimitusketjuriskien huomioiminen, verkkorikollisuuden ja valtiollisten toimijoiden merkityksen ja uhkien ymmärtäminen, sekä riittävän nopea hyökkäysten tunnistus ja niihin reagointi, sekä yleisesti hyvä havainnointikyvykkyys tulivat vahvasti esille varsinkin Flyktmanin ja Rouskun puolelta. Kimmo Rousku nosti esiin tässä vaiheessa myös organisaatioiden erot reagointikyvykkyydessä; ”*Kaikista tärkein kyvykkyys on se, että organisaatio pystyy tunnistamaan ja reagoimaan heihin kohdistuvaan tietomurtoyritykseen mahdollisimman aikaisessa vaiheessa. Todella moni organisaatio on tällä hetkellä siinä tilanteessa, että vasta kun media saa tietää, että nyt tuolla meillä on jotain ongelmia, organisaatio havahtuu tietomurtoon..*”

Suvi Lampila toi esiin erittäin käytännönläheisen esimerkin siitä mitä organisaatioiden tulisi ottaa huomioon varautumisessaan: Organisaation byrokratian. Tällä hän tarkoitti, että vaikka varautumissuunnitelmat olisi tehty paperille vasteaikavaatimuksineen, niin jos niissä ei ole huomioitu sisäisten prosessien

viemää aikaa eivät vasteajat ole tällöin realistisia. "*Organisaatioilla on tiettyjä sääntöjä. Tässä tulee iso kontrasti. Jokin asia pitää korjata ja vaikka sille olisi annettu Top Priority ja budjetti, lopputulema saattaa olla silti se, että odotetaan jotakin byrokraattista steppiä. Esimerkiksi että joku aukaisee vaikka palomuurin portin. Teknisesti muutamien sekuntien / minuuttien homma. Byrokraattisesti se voi olla kuukausien ongelma. On ne hyvät suunnitelmat, mutta se ei paljon lämmitä, jos ei sitä pystytä tuomaan käytäntöön*."

Tämä oli mielenkiintoinen nosto, sillä usein organisaatioissa voidaan ajatella, että omat normaaliin toimintaan liittyvät prosessit menevät kyllä sujuvasti, mutta näin ei välttämättä ole, eikä näitä ole aina sisällytetty varautumissuunnitelmiin. "*Teknologia ei välttämättä ole se pullonkaula vaan se on se byrokratia*." (Lampila).

Harjoittelun merkitystä korostivat varsinkin Flyktman, Karlamaa sekä Rousku, haastatteluissaan. Suvi Lampila nosti tähän kriittisen huomion, että harjoittelu- ja testaustilanteet eivät kuitenkaan vastaa usein sitä todellista tilannetta, eli vaikka harjoiteltaisiin, ei se ole verrattavissa oikeaan tapahtumaan. Tähän aiheeseen Kimmo Rousku nosti omassa haastattelussaan esiin DVV:n järjestämät vuosittaiset Taisto-harjoitukset, jotka ovat kasvattaneet suosiotaan organisaatioiden keskuudessa osallistujamäärän tuplaannuttua vuosien varrella. Nämä harjoitukset keskittyvät ajankohtaisiin uhkiin ja tarjoavat organisaatioille mahdollisuuden testata kyvykkyyksiään hallitussa ympäristössä kattavasti. Koska ihmistekijä nostetaan aina hyvin korkealle riskitekijänä, niin harjoittelun merkitystä ei voi väheksyä. Vaikka Lampilan kritiikki on paikkansapitävä, että harvoin harjoitustilanteissa saadaan testattua kaikkea mitä oikeassa tilanteessa tapahtuisi, niin siltikin harjoitukset antavat käsitystä uhkista, prosesseista, kehittämistarpeista, ja valmistavat ihmisiä ainakin osittain oikeisiin tilanteisiin. Rouskun kiteytyksen mukaan; "*Jos sitä ei ole harjoiteltu, sitä ei ole olemassa*".

Käsiteltäessä merkittävimpiä uhkia organisaatioille nyt ja tulevaisuudessa toistuivat monet samat asiat, kuin aiemmin käsiteltäessä huomioon otettavia asioita ja priorisointia. Toimitusketjujen aiheuttamat uhat ja niiden huomioiminen nousivat vahvasti esille kaikkien haastateltavien puolelta, tai ne vähintään huomioitiin pakollisena osana jatkuvuudenhallintaa. Nähtiin selvästi, että ei ole riittävää huolehtia vain omasta organisaatiosta, sekä se, että toimitusketju-uhkien hahmottaminen, sekä niihin varautuminen ovat usein heikoimpia lenkkejä organisaatioissa. Myös tämä löydös oli yhtenevä sekä kirjallisuuskatsauksen että kyselyn tulosten kanssa. Tämän lisäksi esiin nousivat Flyktmanin puolelta kybervakoilu ja kybersabotaasit, sekä kvanttilaskenta uhkana ja mahdollisuutena. Karlamaa nosti toimitusketjujen lisäksi ihmistekijän perustaen näkemyksensä siihen, että rikolliset käyttävät eniten helppoja keinoja, ja ihmistekijä on eräs suurimmista heikkouksista ketjussa. Kolmantena Karlamaa nosti esiin tekoälyavusteiset haittaohjelmat. Rousku nosti Flyktmanin lailla esiin verkkorikollisuuden ja valtiolliset toimijat, sekä tämän lisäksi tekniset häiriöt digitalisoituvassa maailmassa.

Tulevaisuuden uhista ja teknologioista puhuttaessa päällimmäisenä ja toistuvimpana oli tekoäly, sen uhat ja mahdollisuudet, ja sen mahdollistamat asiat muiden teknologioiden, sekä nykyisten uhkien tehostajana ja kehittäjänä. Automatisaatio, integraatiot, skaalautuvuus, kattavuus, yhdistäminen muuhun teknologiaan (varsinkin kvanttilaskentaan), sekä käyttäjähuijausten tehostuminen

olivat päällimmäisiä keskustelunaiheita. Varsinkin Karlamaa, Lampila ja Rousku toivat esiin myös aspektin, että meille ei ole selvää mitä kaikkea tekoäly voi mahdollistaa tulevaisuudessa, ja mihin teknologinen kokonaiskenttä kehittyy. Se on monissa suhteissa musta aukko. Myös tekoäly yhdistettynä kvanttiteknologiaan ja supertietokoneisiin voi aiheuttaa mm. Rouskun seuraavan uhkakuvan; *"Verkkorikollisorganisaatio saa toteutettua globaalin CMDB -tietovarannon, jossa on kaikki maailman IP osoitteet ja niiden takana olevat tekniset laitteet"…"ja sitten alkavat ylläpitämään sitä versio- ja päivitystietoa niin, että se on mahdollisimman hyvin ajan tasalla, jolloin kun tulee haavoittuvuusilmoitus, niin heti tiedetään tarkalleen ne kaikki maailman miljoonat IP osoitteet johon kannattaa sitten lähettää se tekoälypohjainen botti tekemään tietomurtoa."*. Rousku nosti esiin myös mm. tekoälyyn liittyvän robotisaation ja sen tuomat aivan uudenlaiset uhat varautumiseen liittyen siinä vaiheessa, kun robotteja aletaan käyttää laajemmin. Muista tekoälyyn liittyvistä aspekteista Karlamaa mainitsi mm. metaversen ja XR:n (extended reality) virtuaalitodellisuuteen liittyviä, jo teollisuudessa käyttöönotettuja ja koko ajan laajenevia sovellusmahdollisuuksia. Tekoälyn ja koneiden kehittyessä nämä tulevat laajenemaan käytössä muillekin osa-alueille.

Suvi Lampilan kanssa keskityttiin tarkemmin kvanttiteknologian uhkiin ja mahdollisuuksiin. Hän näki kvanttiuhat hyvin merkittävinä tulevaisuudessa, ja varsinkin kvanttiturvallisen kryptografian kehittämisen tärkeyden niiltä suojautumisessa. Lampila käsitteli aiemmin esiin nostettua NIST-standardia, sekä siihen valittuja algoritmeja ja niiden haasteita. Nyt algoritmeja jouduttiin valitsemaan useita, koska ei pystytä vielä päättelemään mitkä ovat sopivimpia. Työ jatkuu tämän osalta. Haasteena kvanttiturvallisissa algoritmeissa on kuitenkin, että ne eivät aina ole kovin käyttökelpoisia, vaikka ne olisivat turvallisia. Osa kvanttiturvallisista algoritmeista kuten Classic McEliece on niin isoja, että niitä ei voi käyttää tehokkaasti. *"Se, että jokin on kvanttiturvallinen ei tee siitä välttämättä käytännöllistä."*. Tämä on ongelma, jota ratkaistaan ja josta opitaan koko ajan, eli mitkä algoritmit soveltuvat mihinkin käyttöön ja kuinka turvallisia ne ovat.

Tähän liittyen Lampila nosti esiin myös haasteen, joka koskee hyvin monia organisaatioita, eli järjestelmät ja laitteet ("legacy") joita ei ole millään tavalla kehitetty tukemaan kvanttiteknologiaa tai sen uhilta suojautumista. Tämä asettaa tarpeen jatkossa joko viimeinkin uusia vanhat järjestelmät (joka nähtiin myös mahdollisuutena). Lampila kuvasi kyseistä haastetta sekä uhkana että mahdollisuutena; *"Ollaan oikeasti ensimmäistä kertaa sellaisessa tilanteessa 30 vuoteen, että täytyy katsoa asioita"…"On pakko koskea johonkin, joka on pyörinyt siellä iät ja ajat ja ehkä vähän unohduksissa, joku järjestelmä, jonka joku on aikanaan tehnyt ja josta kukaan ei tiedä. Tässä on toisaalta se mahdollisuus, että voidaan tuoda näitä enemmän nykypäivään. Oikeasti tehdä valinta, että ei ruveta korjaamaan vanhaa vaan hoidetaan ihan jollakin uudella modernilla tavalla."*. Lampila nosti esiin kuitenkin myös, että jos järjestelmää ei ole mahdollista eri syistä vaihtaa tai päivittää, niin se voidaan tehdä kvanttiturvallisilla yhteyksillä ja järjestelmä itsessään mahdollisuuksien mukaan ainakin kvanttiärsyttävästi salaten (=ei kvanttiturvallinen, mutta hybridi, jossa käytetään klassisia ja mahdollista kvanttialgoritmia). Myös Karlamaa nosti esiin organisaatioiden teknologiavelan sekä tarpeen arvioida missä määrin tätä on jo hoidettu. Tähän liittyivät myös pilvialustat, joka nähtiin jo toteutuneena trendinä,

mutta myös harkinnanvaraisena onko niiden käyttöön siirtyminen aina paras vaihtoehto, vai onko joko ns. pilven reunalla, tai omissa konesaleissa datan käsittely kuitenkin ajoittain perusteltu ratkaisu. Tämän ajatuksen toi esiin varsinkin Flyktman. Tämän hetken käytännöt varsinkin kriittisissä organisaatioissa tukevat tätä ajatusmallia, sillä osa ohjeistuksista ja standardeista ei vielä tue kokonaan pilvisiirtymää, vaan paikallisempaa hallintaa.

Haastateltavat nostivat vahvasti esiin sen, että sillä datalla, joka on luotu aiemmin, on arvoa vielä vuosikymmenienkin päästä. Flyktman nosti tämän hyvin esiin; ”*Jos organisaation salaama tieto on relevanttia vielä kahdenkymmenen vuoden päästä, ja kahdenkymmenen vuoden päästä se salaus pystytään purkamaan, niin se tarkoittaa sitä, että tänään pitää alkaa salaamaan kvanttiturvallisesti.*” Tämä antoi melko hyvän kuvan ongelmaan, että vaikka osa tulevista teknologioista voi olla arkipäivää vasta tulevaisuudessa 5-30 vuoden aikajänteellä, niin se tieto mitä nyt on olemassa vaatii suojaamista vielä silloinkin, joka tarkoittaa, että meidän pitää olla tuleviin uhkiin nähden hyvin paljon etuottoisia suojaustoimissamme. Karlamaa puhui ”kvantti-inventaariosta”, eli tunnistamisesta missä kaikkialla meillä on sellaisia järjestelmiä jne., jotka pitää suojata kvanttiteknologiaa vastaan.

6G:n merkittävyys jakoi jonkin verran mielipiteitä siihen vastanneiden haastateltavien keskuudessa. Osittain se nähtiin lähinnä seuraavana askeleena tietoliikennetekniikassa, joka toki mahdollistaa paljon, mutta on enemmän asiantuntijoille näkyvää, kun taas osittain se nähtiin monin osin vielä hämärän peitossa olevana palvelualustana, jonka vaikutukset ja uhat yhdistettynä muihin teknologioihin voivat olla hyvinkin mullistavat. Flyktman toi esiin tässä yhteydessä digitaaliset kaksoset sekä näihin liittyvänä 6G.n mahdollistaman sensoritietomäärän välittämisen ja käsittelyn, joiden avulla nämä saataisiin aivan toisella tavalla käyttöön kuin nykyisin. Tämä nähtiin sekä uhkana että mahdollisuutena.

Rousku ja Flyktman toivat esille huomion sähköverkosta ja energiatuotannosta yleensä. Molemmat näkivät, että tämä, turvaaminen ja riittävyyden varmistaminen ovat asioita, joihin tulee keskittyä jatkuvuudenhallinnan kannalta. Flyktman huomioi, että nykyiset teknologiat kuten tekoäly vievät huomattavasti energiaa, ja niiden kehittämiseen energiatehokkaammiksi tulee panostaa. Kvanttilaskennan yksi mahdollinen hyöty on parantaa olennaisesti laskennan energiatehokkuutta. Vaikka itse sähköntuotantoon eivät organisaatiot voikaan suoraan vaikuttaa, niin ne voivat huolehtia varautumisestaan, ja huomioida myös laitteidensa ja toimintojensa energiankulutuksen. Akkuteknologian kehitys ja sen mahdollisuudet varautumisessa nostettiin esiin Rouskun puolelta.

Kaikkien haastateltavien kesken teknologioista tekoäly ja kvanttiteknologia olivat merkittävimmät, joihin on pakko keskittyä. Rousku nosti myös esille robotisaation merkityksen; "*Vaikka tekoälykehitys tuntuu olevan tällä hetkellä se kaikista merkittävin muutostekijä, meidän tulisi kuitenkin varautua siihen, millainen globaali yhteiskunnallinen disruptiivinen muutos tulee palvelurobotisaatiosta, joka hyödyntää silloin yleisen tekoälyn (AGI) tasoa lähestyvää tekoälyteknologiaa kehittyvien fyysisten robottien käyttöliittymänä ja ohjaajana.*"

Keskusteltaessa organisaatioille tärkeimmistä työkaluista ja prosesseista sekä kyberturvallisuuden hyödyntämisestä jatkuvuudenhallinnassa

haastateltavien vastaukset peilasivat hyvin suojattavaa omaisuutta ja tunnistettuja uhkia käsitteleviä osuuksia jotka tulivat esiin jo organisaatioiden varautumisen toimenpiteitä ja priorisointia käsittelevissä kysymyksissä (kriittisten toimintojen tunnistamisen merkitys, priorisointi, johdon rooli kokonaisuudessaan, sekä riskinhallintalähtöinen ja ennakoiva toiminta kaiken pohjana). Varsinkin Karlamaa painotti riskienhallinnan perustavanlaatuista merkitystä; "*kyberturvallisuus on osa riskienhallintaa*"…"*Loppupeleissä kauneimmillaan ja paljaimmillaan se on organisaatioiden ja yritysten riskienhallintakyvykkyyttä toimia oikein tilanteessa, arvioida kyvykkyydet, arvioida omat kriittiset suojattavat kohteet, tehdä niille varautuminen, ja valmius johtaa sitä organisaatiota valmiilla olemassa olevilla malleilla. Kun jotain sattuu, niin kaikki toimii.*". Tällä painotettiin, että kyberturvallisuus ja jatkuvuudenhallinta eivät ole erillisiä osa-alueita, vaan riskienhallinnan pitäisi olla kaiken toiminnan perusta, johon nämä osa-alueet kuuluvat.

Karlamaa, Lampila ja Rousku toivat esiin tässäkin regulaation ja standardien merkitystä. Ei vain pakottavina vaatimuksina, vaan varsinkin standardeja ja viitekehyksiä ohjaavina parhaina käytäntöinä, joista organisaatiot voivat ottaa itselleen merkityksellisimmät osaksi toimintaansa. Lampila nosti esiin varsinkin tulevan amerikkalaisen NIST:n kvanttisalauksen standardin, joka määrittää kvanttiturvallisia algoritmeja. Tämän haasteena nähtiin, että siinä missä aiemmin salausmenetelmiä oli vain muutama, nyt niitä jouduttiin ottamaan mukaan useampia, koska aihealue on vasta kehitysvaiheessa. Tällä hetkellä kuitenkin kvanttiteknologiaan ja sen uhkilta suojautumiseen pyritään varautumaan jo ennakoivasti lainsäädännöllä ja standardeilla. Flyktman ja Rousku mainitsivat molemmat valvomot, jotka tekevät havainnointia 24/7. Nämä tunnistettiin olevan hintansa vuoksi mahdottomia osalle organisaatioista, mutta varsinkin Rousku toivoi, että tähän tekoäly saattaisi tuoda ratkaisua tulevaisuudessa esim. virtuaalisten kybervalvomoiden kautta. Erikseen mainittiin myös varmuuskopiointi, järjestelmien koventaminen, havainnointikyvykkyys, järjestelmäinventaariot, sekä jälleen osaaminen, koulutukset, harjoitukset, ja testaaminen. Lampila toi esiin haastattelussaan myös nollaluottamus (zero-trust) -arkkitehtuurin, jossa luovutaan normaaleista pitkäaikaisista käyttöoikeuksista, ja keskitytään kertakäyttöisiin, aina erikseen varmistettaviin oikeuksiin, jolloin pystytään poistamaan hyökkäyspinta-alaa ja vähentämään mm. identiteettien ja käyttäjäoikeuksien väärinkäyttöön kohdistuvia riskejä.

Haastattelujen osalta tulle huomioida, että vaikka haastateltava ei olisi itse haastattelussa painottanut jotain asiaa, niin se ei tarkoita, etteikö hän voisi nähdä sitä merkityksellisenä. Haastattelujen haaste on aina, varsinkin, kun käsiteltiin laajaa kokonaisuutta, että ne ovat senhetkisen keskustelun tuotoksia, eivätkä anna syväluotaavaa kokonaiskuvaa haastateltavan näkemyksistä tai osa-alueesta. Varsinkin, kun tutkimusraporttiin jouduttiin referoimaan materiaalia.

7.2 Tutkimuksen luotettavuus

Tutkimuksessa käytettiin laaja-alaisesti tutkimusmateriaalia, ja sitä pyrittiin keräämään monipuolisesti eri tahoilta huomioiden silti lähteen luotettavuus. Kirjallisuuslähteissä pyrittiin käyttämään asiantuntijalähteitä, joilla on tunnettuutta alalla, mutta ajoittain myös yksittäisiä asiantuntijalähteitä käytettiin. Voidaan siis argumentoida, että kirjallinen lähdemateriaali ei ole tutkimustietoa, mutta tämä on asia joka voimakkaasti kehittyvällä kyberturvallisuuden alalla on tyypillistä, samoin kuin se, että tutkimusaiheena olivat myös tulevat trendit, ei jo aiemmin tutkittu ja toteutunut tieto.

Ristiintarkastusta saatiin sekä kyselyn, että haastattelujen kautta. Kyselyyn vastanneiden määrä jäi melko suppeaksi (27), mutta koska kysely kohdistettiin selkeästi asiantuntijoille, jaettiin vain rajatusti suomen kieltä puhuvien asiantuntijoiden käyttämillä kanavilla, ja laajimmillaan LinkedInissä oli jo etukäteen oletettavaa, että vastausmäärä jäisi pienemmäksi. Kysely ei ollut siis laajuudeltaan tieteellisesti kattava, mutta se antoi silti avoimine kyselyosioineen vertailukelpoista tietoa tutkimusaiheeseen. Kun myös huomioidaan, että kyselyn tulokset eivät olleet voimakkaassa ristiriidassa kirjallisuuskatsauksen ja haastattelujen kanssa koettiin kyselyn anti tutkimusta rikastuttavaksi.

Haastattelujen avulla saatiin erittäin hyvää laadullista informaatiota aiheeseen liittyen. Kaikki haastateltavat ovat asiantuntijoita aloillaan, ja koska haastattelussa erikseen painotettiin, että heidän ei tarvitse ottaa kantaa aiheisiin, jotka eivät ole heidän osaamisalueellaan voidaan haastattelun tuloksia pitää luotettavina. Litterointia katsottaessa ei myöskään ollut nähtävissä, että haastattelija olisi ohjannut haastateltavia tietyntyyppisiin vastauksiin.

Yksi tutkimuksen luotettavuutta ja käyttökelpoisuutta heikentävä tekijä on, että aihetta jouduttiin sen prosessin aikana todetun laajuuden vuoksi käsittelemään pintapuolisemmin. Huomiointivaiheessa rajaaminen ei kuitenkaan enää ollut järkevää, joten hyväksyttiin se, että asioita ei voitu tässä tutkimuksessa käsitellä syvällisemmin, vaan tämä pitää jättää mahdollisiin tuleviin tutkimuksiin.

7.3 Tulokset

Tarkempaa pohdintaa tutkimukseen liittyen käsitellään seuraavassa kappaleessa, tässä käydään läpi tutkimuskysymysten vastaukset lyhyemmin. Kappaleessa käydään läpi ensin alakysymykset, ja sitten näiden yhteenvetona pääkysymys.

a. Mitkä ovat merkittävimpiä kyberuhkia organisaatioille nyt ja tulevaisuudessa?

Merkittävimmiksi kyberuhkiksi organisaatioille nostettiin nykyisistä uhkista ihmistekijä, palvelunestohyökkäykset, haittaohjelmat (sisältäen kiristyshaittaohjelmat), toimitusketjuihin kohdistuvat uhkat, valtiollisen tason kyberuhat, haavoittuvuudet, pilvipalveluihin kohdistuvat hyökkäykset,

käyttäjäoikeuksiin kohdistuvat hyökkäykset, hallinnoimattomat (usein myös vanhat) laitteet ja alustat, hyökkääjien piiloutuminen järjestelmiin ja lateraalinen liikkuminen sisällä (myös LOTL ja LOTS), sekä tekoäly osana hyökkäyksiä. Nousevista uhkista merkittävimpiä olivat varsinkin tekoälyyn ja sen kehittymiseen ja kvanttiteknologiaan liittyvät uhat edellä mainittujen ohella.

b. *Onko kybermaailman aiheuttamat uhat tunnistettu riittävän hyvin organisaatioissa ja turvaavat toimenpiteet toteutettu?*

Tähän vastattiin sekä kyselyn että haastatteluiden perusteella, ja tuloksena oli, että varsinkin reguloiduissa organisaatioissa ja aloilla uhat ja varautuminen ovat melko hyvällä tasolla, mutta näidenkin välillä on hajontaa. Mitä pienempi tai vähemmän reguloitu organisaatio / ala on, sitä enemmän vaihtelua. Otannan suppeuden vuoksi tähän ei voida vastata kuin suuntaa antavasti. Vaikka kyselyn tulokset olivat osittain ristiriidassa organisaatioiden kokoja vertaillessa, niin uhkien tunnistaminen oli vahvempaa kuin keinojen implementointi kaikissa organisaatiotyypeissä.

c. *Mikä on organisaatioiden arvioitu kyky vastata jatkuvuutta vaarantaviin kyberuhkiin?*

Tämän vastaus oli melko yhtenevä alakysymyksen b. kanssa. Tässä kuitenkin merkittävämmäksi tekijäksi nousi myös organisaation koko joka vaikuttaa suoraan resursseihin. Silti regulaatio oli tässäkin määräävin tekijä. Tässä näkyi myös selvemmin erot organisaatioiden kokoja vertaillessa.

d. *Kyberturvallisuuden avulla voidaan tehostaa jatkuvuudenhallintaa nykyisestään organisaatioissa?*

Vastaus tähän alakysymykseen nivoutui hyvin paljon myös muihin kuin kyberturvallisuuden teknisiin keinoihin, mikä oli positiivinen löydös. Kyberturvallisuutta ei nähty tutkimusmateriaalien mukaan pelkästään teknisinä suojauskeinoina, vaan pääosin osana organisaation kokonaisturvallisuuden hallintaa. Tässä esiin nousivat johdon rooli, kokonaisvaltainen, ennakoiva riskienhallinta, kyberturvallisuuden standardit ja viitekehykset, sekä ohjaava regulaatio, ihmistekijän huomioiminen (harjoittelu, testaaminen, koulutukset). Tämän lisäksi huomioitiin kappaleessa 3.3.4. esitettyjä teknisiä keinoja

Vastaus pääkysymykseen "*Miten merkittävimmät ja nousevat kyberuhat tunnistetaan ja huomioidaan osana jatkuvuudenhallintaa ja miten näihin varautumista voitaisiin tehostaa*?" voitaisiin kiteyttää siihen, että mitä reguloidumpi ala ja / tai suurempi organisaatio sen paremmin uhat tunnistetaan osana kokonaishallintaa. Organisaatioiden joukossa on silti merkittävää hajontaa, ja pääosin nousevat uhat tunnistetaan huonommin kuin tämänhetkiset. Kuitenkaan se, että uhat oli

tunnistettu, ei välttämättä johtanut toimenpiteiden implementointiin, ellei siihen ollut pakottavaa syytä, joka usein oli lakien tuomat vaatimukset.

Kiteytettäessä tutkimuksen pohjalta nousseet huomiot vastattaessa päätutkimuskysymykseen muutamalla lauseeseella kaikkien löydösten perusteella, niin; Organisaation johdon tulisi sitoutua jatkuvuudenhallintaan ja nähdä kyberturvallisuus osana sitä. Organisaation toiminnan tulisi aina pohjautua kokonaisvaltaiseen, ennakoivaan riskienhallintaan osana toimintaansa jossa kyberturvallisuus ja jatkuvuudenhallinta ovat osa kokonaisuutta eivätkä omissa siiloissaan, ja kriittisimmät suojattavat toiminnot on tunnistettu. Organisaation tulisi lisäksi kouluttaa henkilöstöään ja parantaa näiden osaamista, sekä käyttää teknologisia keinoja suojelemaan itseään niin sisäisiltä kuin ulkosilta uhkilta, priorisoiden toimintansa kriittisimmän ytimen turvaaminen, sekä varautua aina siihen, että jotain tapahtuu.

7.4 Yhteenveto ja pohdinta

Tässä osiossa vedetään yhteen tutkimuksen kokonaisanalyysi ja johtopäätökset. Aihetta tutkittiin kirjallisuuskatsauksen, kyselyn ja haastattelujen kautta. Tavoitteena oli vastata tutkimuskysymyksiin alakysymyksineen, sekä saada tietoa, jonka avulla organisaatiot voivat priorisoida kyberturvallisuuden toimenpiteitään tehostaakseen jatkuvuudenhallintaansa.

Tarkasteltaessa kyberturvallisuuteen ja jatkuvuudenhallintaan kohdistuvia uhkia, sekä molempien vaatimuksia on selkeästi osoitettavissa, että nykyisessä digitaalisessa maailmassa jatkuvuudenhallintaa ja kyberturvallisuutta ei voi erottaa toisistaan. Tämä tuli selväksi teoriatasolla tarkasteltaessa kappaleiden 2–3 löydöksiä, sekä myös vahvasti esiin haastatteluiden ja kyselyn perusteella. Näyttää siltä, että organisaatiot ovat ymmärtäneet nykymaailmassa kyllä kyberturvallisuuden merkityksen jatkuvuudenhallinnan osana, mutta toimenpiteiden implementointi on vielä monin osin kesken. Organisaatioiden tulisi myös hahmottaa paremmin, että vaikka monet kyberuhat itsessään ovat teknisempiä, ja kohdistuvat digitaaliseen toimintaympäristöön, niin kyberturvallisuus ja keinot kyberuhkilta suojautumiseen ei sitä läheskään aina ole, vaan se on kokonaisuus joka muodostuu mm. ihmisistä ja heidän toiminnastaan, organisaation hallinnasta ja fyysistä suojaustoimenpiteistä teknisten suojausratkaisuiden lisäksi. Monesti kyberturvallisuus ei siis ole niin teknistä ja vaikeasti ymmärrettävää, kuin monesti tunnutaan ajattelevan edistäen siiloutumista.

Ihmistekijä oli se, joka nostettiin jo kirjallisuuskatsauksen perusteella merkittävimmäksi uhkaksi, se nousi esiin kyselyssä, ja tuli esiin myös haastatteluissa. Tämän uhkan merkittävyys piilee siinä, että se on, tai voi olla osana niin monessa erilaisessa uhassa. Ihmistekijä uhkana ei rajoitu pelkästään huijauksiin (sosiaalinen manipulointi, tietojen kalastelu, petokset), vaan se voi realisoitua pelkästään tahattoman virheen tai tahallisen teon kautta, liittyä toimittajiin, resursseihin, organisaation käytäntöihin jne. Harva uhka on kokonaan teknologinen, jossa ihmistekijällä ei olisi mitään osuutta. Tähän tehokkaina keinoina kaikin puolin

annettiin harjoittelu ja osaamisen parantaminen, sekä toimintojen testaaminen. Tämä on paitsi kustannustehokasta, eikä näin ollen niin organisaation koosta riippuvaa, niin myös sitä perustavaksi lähtökohdaksi nostettua asiaa, eli riskienhallintaa parantavaa. Osaava henkilö pystyy paremmin tunnistamaan organisaatioon kohdistuvat riskit ja tuomaan ne johdon tietoon, eikä vain välttämään hyökkäyksiä. Erääksi ohjaavaksi pohdinnaksi nousi, miten suuri merkitys ihmisillä on kyberturvallisuuden osana. Jos ihmiset ovatkin suurin uhka, niin meillä on potentiaali olla myös merkittävin turvaava tekijä, jolla on suurin vaikutus ainakin tällä hetkellä.

Josta päästään seuraaviin kriittisimmiksi nostettuihin huomioihin tutkimuksessa, eli Johdon rooliin, sekä riskienhallintaan kaiken perustana. Tämä tuli esiin kirjallisuuskatsauksessa sekä haastatteluissa selvimmin. Jatkuvuudenhallinta ja kyberturvallisuus sen osana eivät ole vain yksittäisten asiantuntijoiden työtä, vaan johdolla pitää olla asian omistajuus ja käsitys asian merkittävyydestä, joka ohjautuu teoiksi, johtamiseksi, ja resursoinniksi. Tämä voidaan saada aikaan sillä, että organisaatioiden johto integroi kokonaisvaltaisen, ennakoivan riskienhallinnan osaksi päivittäistä toimintaansa, jonka osana on asiantuntijoita johtotasolla asti syöttämässä tilannetietoa, eivätkä siiloutuneena omiksi tiimeikseen teknisinä- tai prosessisuorittajina. Harva asia voi toimia, jos sille ei ole johdon tukea ja näillä ymmärrystä mitä asia merkitsee ja voi aiheuttaa. Ennakoivalla riskienhallinnalla tarkoitetaan juuri tutkimusmateriaalien perusteella sitä, että toiminta ei ole reaktiivista, vaan juuri tulevat uhkat huomioivaa ja ennakoivaa, jolloin toimenpiteisiin voidaan ryhtyä proaktiivisesti. Tätä pyritään nyt ohjaamaan ennakoivalla regulaatiolla nousevien teknologioiden osalta.

Tästä päästään seuraavaan merkittävään asiaan, joka nousi materiaaleista esiin, eli ”tehdään kun on pakko” -asenne. Tällä tarkoitetaan, että jos organisaatiota ohjaa regulaatio, tai se on velvoitettu noudattamaan standardisointeja, suoriutuminen on paremmalla tasolla, kuin reguloimattomissa. Tämä ei sinällään ole yllättävää, mutta voidaan pitää kuitenkin erikoisena, että organisaatiot eivät ilman pakkokeinoja suojaa kriittisiä resurssejaan ja toimintojaan, vaikka ne ovat niiden jatkuvuuden edellytys. Tässä voi olla osittain kyse myös tietämättömyydestä tai ymmärtämättömyydestä, mutta myös reaktiivisesta ajattelusta, ja ehkä ajatusmallista, että heille ei käy mitään / he eivät kiinnosta hyökkääjiä. Kuitenkin nykymaailman verkottuneessa yhteiskunnassa on hyvin vaikea tutkimusmateriaaliakin tarkastellessa enää hahmottaa missä vaikuttavuussuhteet menevät, ja ketkä oikeastaan ovat sitä hyökkäyspinta-alaa toimijoina. Tämä kytkeytyy suoraan nyt niin kyselyissä, haastatteluissa, kuin kirjallisuuskatsauksessa merkittäväksi koettuun uhkaan, tai organisaatioiden heikoimpana nähtyyn osa-alueeseen, eli toimittajaketjuriskeihin ja niiden hallintaan. Monet organisaatiot eivät edes tiedosta kuinka moneen portaaseen heidän hankintaketjunsa yltävät, minne kaikkialle heidän tietonsa voivat tietomurtotilanteessa päätyä, ja mitä rajapintoja heiltä löytyy toimittajiin.

Kun tarkasteltiin tutkimusmateriaalien julkishallinnon ja huoltovarmuuskriittisille organisaatioille tehtyjä tutkimuksia, niin niistä voitiin nähdä erot jo toimialojen sisäisessä, sekä niiden välisessä tilanteessa. DVV:n vuoden 2023

kyselyn keskiarvo oli n. 0,7 (1 ollessa paras). Kyselyssä oli myös eroteltu toiminnan jatkuvuus ja varautuminen sekä kyberturvallisuus, mikä on kyselyteknisesti järkevää, mutta nostaa esiin myös sen, että sitä ei ehkä nähdä niin selkeästi osana jatkuvuudenhallintaa. HVK:n kyberkypsyyden arvioinnissa vuonna 2022 keskiarvo oli 3 (5 ollessa paras). Vaikka kummankaan tutkimuksen tulokset eivät ole hälyttäviä millään tavalla niin näidenkin osalta tulee muistaa, että ketju on niin vahva kuin sen heikoin lenkki. Ja tutkimuksessa tuli esiin monia heikoimpia lenkkejä, jotka ovat usein esim. ihmistekijä, toimitusketjuhallinta, hyökkäykseen reagoinnin viive, tai johdon sitoutuminen (esim. riittämättömät resurssit).

Nousevien teknologioiden osalta jokaisen organisaation tulisi alkaa valmistautua ainakin tekoälyn ja kvanttiteknologian tuomiin uhkiin, mutta myös hyväksikäyttää vastuullisesti mahdollisuuksia. Tässä nousee eteen taas se ennakoivuus. Data pitää suojata jo nyt, koska se voi olla relevanttia vielä vuosikymmenten päästä, ja tekoäly kehittyy niin nopeasti, että sitä voidaan jo käyttää koko ajan tehokkaammin hyökkäyksissä (mutta myös puolustuksessa). Nämä teknologiat ovat kaksiteräisiä miekkoja, mutta yhdenkään organisaation ei tulisi jättää niitä vuonna 2024 huomioimatta ajatuksella, että ne eivät ole tätä päivää. Näin ollen organisaatioiden tulisi siis ennakoivasti varautua mm. kvanttiturvallisten salasanojen ja -metodien käyttöön, sekä tekoälyn hyödyntämiseen (turvallisen sovelluskehityksen kautta).

Eräs tutkimuksessa esiin tullut asia oli, että niin nousevat teknologiat, koneiden tehokkuuden kasvaminen, kehittyvät haittaohjelmat, kuin verkkorikollisuuden ammattimaistuminenkin (kyberrikokset palveluna) lyhentävät koko ajan organisaatioiden vasteaikoja reagoida hyökkäyksiin ja niiden vaikutuksiin. Koska kaikilla ei ole mahdollisuuksia omaan tai ostettuun 24/7 valvontaan on sitäkin tärkeämpää varautua muin teknisin keinoin hyökkäyksiin ja toimintojen suojaamiseen, on sitten kyse esim. palomuureista, haavoittuvuuksien hallinnasta, monivaiheisen tunnistautumisen käytöstä, varmuuskopioinnista, tai turvallisista verkkoyhteyksistä. Nämä käsiteltiin tarkemmin luvussa 3.3.4. Tulee kuitenkin huomioida, että jokaisen organisaation tulisi varautua siihen, että järjestelmiin päästään, ei vain keskittyä estämään pääsyä.

Tutkimus ei itsessään tuottanut ehkä merkittävästi täysin uutta tietoa, mutta se avasi tämänhetkistä suomalaista organisaatiokenttää, ja antoi koottua tietoa siitä mitä organisaatioiden tulisi huomioida varautumisessaan, sekä kyberturvallisuuden merkitystä osana kokonaisvaltaista jatkuvuudenhallintaa. Jos siis organisaatioiden edustajat lukevat tutkimuksen he saavat jo vertailtua, ja useista lähteistä kerättyä ja analysoitua tietoa siitä mitkä ovat merkittävimpiä uhkia nyt ja tulevaisuudessa, mihin voimavaroja pitäisi keskittää, ja mikä nähdään tärkeäksi asiantuntijoiden keskuudessa. Tutkimus tuotti myös kyselyn kautta sellaista tietoa mitä ei ole juurikaan organisaatiokentiltä kerätty, eli näkemyksiä jotka eivät kohdistu ainoastaan huoltovarmuuskriittisiin organisaatioihin tai julkisiin toimijoihin. Kokonaisuudessaan tutkimus siis nähdään hyödyttävänä, jos sen tulosten perusteella organisaatiot tekevät ratkaisuja lähestymistapansa tai priorisointiensa suhteen.

7.5 Jatkotutkimuksen tarve

Tutkimuksen suurin haaste kohdistui lopulta tutkimusaiheen laajaan rajaukseen, joka johti siihen, että monia aspekteja ei pystytty käsittelemään syvällisemmin, vaikkakin saatiin kokoava ymmärrys aiheesta tutkimustavoitteen mukaisesti. Jatkotutkimuksen tarve nousee tämän tutkimuksen osa-alueiden syventämisestä, jotta saataisiin tarkempaa tietoa. Mahdollisia tutkimusaiheita olisivat esimerkiksi keskittyminen lähinnä nouseviin uhkiin, ja varsinkin nousevien teknologioiden ristivaikutuksiin, siihen miten ne vaikuttavat toisiinsa. Toinen aihealue olisi tehdä laajempi tutkimus organisaatiokentällä juuri niiden toimitusketjujen parissa, jotka eivät ole suoraan huoltovarmuuden piirissä tämän hetken varautumisesta ja kyberturvallisuuskypsyydestä. Kolmas aihealue nostettiin esiin kyselyn vapaassa sanassa, eli; ”*Paljonko oikeasti resursseja eri kokoiset organisaatiot käyttävät tieto- ja kyberturvallisuuden varmistamiseen. Samalla olisi hyvä tutkia, että miten käytetyt resurssit korreloivat poikkeamien määrään*.”. Tämä olisi myös mielenkiintoinen jatkotutkimusaihe, jolla voitaisiin nähdä mitkä resurssoinnit antavat parhaan vasteen käytetylle rahalle ja ajalle. Tutkijaa itseään kiinnostaa myös 6G :n vaikutukset palvelualustana muille nouseville teknologioille ja sitä kautta nouseville uhkille.

LÄHTEET

Ackerman, R. (2023). *Just Why Are So Many Cyber Breaches Due to Human Error?* Security Today 2.8.2023. https://securitytoday.com/articles/2022/07/30/just-why-are-so-many-cyber-breaches-due-to-human-error.aspx

Aksela, M., Marchal S., Patel, A., Rosenstedt, L. & WithSecure (2022). *Tekoälyn mahdollistamat hyökkäykset*. Traficomin julkaisuja 30/2022. Tekoälyn mahdollistamat kyberhyökkäykset

Amazon Web Services AWS. (2015). *Introduction to AWS Security by Design – A solution to Automate Security, Compliance and Auditing in AWS*. Intro to Security by Design (awsstatic.com)

Amici, J., Asinari, P., Ayerbe E., Barboux P., Bayle-Guillemaud, P., Behm R. J., Berecibar M., Berg E., Bhowmik A., Bodoardo, S., Castelli I. E., Cekic-Laskovic, I., Christensen, R., Clark, S., Diehm, R., Dominko, R., Fichtner, M., Franco A. A., Grimaud, A., (…) Edström, K. (2022). *A Roadmap for Transforming Research to Invent the Batteries of the Future Designed within the European Large Scale Research Initiative BATTERY 2030+*. Advanced Energy Materials 2022, 12, 2102785. https://doi.org/10.1002/aenm.202102785

BSI (2024). *NIS2 to ISO/IEC 27001 Mapping Tool*. bsi-ce-nis2-mapping-tool-de-de-en.pdf

Crowdstrike (2024). *Global Threat Report*. https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

CVE (2024). *Etusivu*. https://www.cve.org/

Digi- ja väestötietovirasto (ei pvm. a). *Mitä on Digiturva?* https://dvv.fi/mita-on-digiturva

Digi- ja väestötietovirasto (2023a). *Organisaation Digiturvakysely – Raportti ja keskeiset havainnot*. Digitalisaatio ja digitaalinen turvallisuus / Erja Kinnunen 30.5.2023 (DVV). https://dvv.fi/documents/16079645/110183105/Organisaation+digiturvakysely,+raportti+kev%C3%A4t+2023.pdf/f8bededb-4702-85d3-2623-fadd5096458d/Organisaation+digiturvakysely,+raportti+kev%C3%A4t+2023.pdf?t=1691566149881

Digi- ja väestötietovirasto (2023b). *Turvallisen sovelluskehityksen käsikirja*. https://wiki.dvv.fi/display/SOVOP

Digi- ja Väestötietovirasto (2024) *Jatkuvuudenhallintamalli*. VAHTI -työryhmä. Yhteinen malli jatkuvuudenhallintaan

Direktiivi 2019/881. *Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvalli suussertifioinnista*. Publications Office

Direktiivi 2022/2555. *EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa*. Publications Office

Edwards, M. (2022). *Mikä on ISO/IEC Tietoturvastandardi?*. Verkkoartikkeli ISMS.online. Saatavilla 20.11.2024. Mikä on ISO/IEC 27001, tietoturvastandardi

Elo, T. (2024). *6G – Lue laaja ja kattava opas tulevaisuuden teknologiaan*. Cryptonews verkkoartikkeli 9.9.2024. Saatavilla 21.11.2024 https://fi.cryptonews.com/guides/6g-opas.htm

Eskola, J., Suoranta, J. (2008). *Johdatus laadulliseen tutkimukseen (8. p.)*. 174-180. Tampere: Vastapaino.

Euroopan komissio (14.10.2024). *AI Act*. Saatavilla 22.11.2024. AI Act | Shaping Europe's digital future

Euroopan komissio C(2024) 7151. *Commission implementing regulation (EU) of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers*. C_2024_7151_F1_COMMISSION_IMPLEMENTING_REGULATION_EN_V4_P1_3633674_9FyMT2pK3VCay0EfRvbpzUHWbLo_109217.PDF

Euroopan komissio C(2024) 7151. *Annex to the commission implementing regulation (EU).*C_2024_7151_F1_ANNEX_EN_V5_P1_3633675_BBlQ0exGHpqQwpwtKKXMcFAQi8s_109218.PDF

Euroopan parlamentin ja neuvoston asetus 2022/868. Euroopan parlamentin ja neuvoston asetus (EU) 2022/868, annettu 30. päivänä toukokuuta 2022, eurooppalaisen datan hallinnoinnista. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022R0868

Euroopan parlamentin ja neuvoston asetus 2024/1689. *Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä*. Publications Office

Euroopan parlamentin ja neuvoston asetus 2022/2554. *Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä*. Publications Office

Euroopan parlamentti (2021). *Massadata: Määritelmä, hyödyt, haasteet (infografiikka)*. Verkkoartikkeli 29.3.2021. Saatavilla 22.11.2024. Massadata: määritelmä, hyödyt, haasteet (infografiikka) | Aiheet | Euroopan parlamentti

Euroopan unionin kyberturvallisuusvirasto ENISA (2024a). *ENISA Threat Landscape 2024*. ENISA Threat Landscape 2024 — ENISA

Euroopan unionin kyberturvallisuusvirasto ENISA (2024b). *ENISA Foresight Cybersecurity Threats 2030*. Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report — ENISA

Euroopan unionin kyberturvallisuusvirasto ENISA (2022). *Suurimmat kyberuhat EU:ssa*. EU:n kyberturvallisuusvirasto tiedot heinäkuu 2021-heinäkuu 2022. https://www.consilium.europa.eu/fi/infographics/cyber-threats-eu/

Eurooppa-neuvosto (2024a). *Kyberturvallisuus: miten EU torjuu kyberuhkia?*. Saatavilla 20.11.2024. https://www.consilium.europa.eu/fi/policies/cybersecurity/

Eurooppa-neuvosto (2024b). *Kyberkestävyyssäädös: neuvostolta uusi laki digitaalisten tuotteiden turvallisuusvaatimuksista.* Lehdistötiedote 10.10.2024. https://www.consilium.europa.eu/fi/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

Faruk, J.H., Tahora, S., Tasnim, M., Shahriar, H., Sakib, N. (2022). *A review of Quantum Cybersecurity: Threats, Risks and Opportunities. Conference on AI in Cybersecurity (ICAIC) 24.-26-5-2022.* Konferenssijulkaisu. A Review of Quantum Cybersecurity: Threats, Risks and Opportunities | IEEE Conference Publication | IEEE Xplore

Fingrid (2022). *Venäjältä tuotu sähkö Suomessa*. Saatavilla 22.11.2024. https://www.fingrid.fi/globalassets/dokumentit/fi/kantaverkko/suomen-sahkojarjestelma/ajankohtaista05042022_sahkontuonti.pdf

Fingrid (2023). *Esittelytilaisuus sähkötehon riittävyys selvityksestä*. Fingridin esittelytilaisuus 13.6.2023. PowerPoint Presentation

Folorunsho, O., Ayinde, A., Olagoke, M. ja Fatoye, O. (2019). *Evaluating Cybersecurity Theories, Models, Standards and Frameworks*. Journal of Behavioral Informatics – Digital Humanities & Development Research. 5(4). joulukuu 2019. http://dx.doi.org/10.22624/AIMS/BHI/V5N4P7

F-Secure (ei pvm.). *Mitä on kyberturvallisuus?*. Saatavilla 20.11.2024. Mitä on kyberturvallisuus? | F-Secure (f-secure.com)

Geeksforgeeks (2024). *What is Artificial Intelligence?*. verkkoartikkeli 21.8.2024. Saatavilla 22.11.2024. What is Artificial Intelligence? - GeeksforGeeks

Guo, H. & Yu, X. (2022). *A Survey on blockchain technology and its security*. Blockchain: Research and Applications 3(2) kesäkuu 2022. https://doi.org/10.1016/j.bcra.2022.100067

Helsingius, M. (2017). *Kvanttilaskenta ja kyberturvallisuus*. Puolustusvoimien tutkimuslaitos. Tutkimuskatsaus 01-2017. . https://puolustusvoimat.fi/documents/1948673/2104503/PVTUTKL+Tutkimuskatsaus+1-2017.pdf/fc2dd702-919f-4395-a385-0fc391525ff8/PVTUTKL+Tutkimuskatsaus+1-2017.pdf?t=1494503092000

Huoltovarmuuskeskus HVK (ei pvm.). *Jatkuvuudenhallinta*. Saatavilla 21.11.2022. Jatkuvuudenhallinta - Huoltovarmuuskeskus

Huoltovarmuuskeskus (2022). *Toimialojen kyberkypsyyden selvitys 2022 – Kansallinen koosteraportti*. Huoltovarmuuskeskuksen julkaisu. hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

Hyvärinen, M., Suoninen, E., Vuori, J. (2021). *Haastattelut*. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Saatavilla 22.11.2024. Haastattelut - Tietoarkisto (tuni.fi)

IBM (2023). *Cost of Data Breach Report 2023*. https://www.ibm.com/reports/data-breach

ICC International Chamber of Commerce (2016). *Tietoturvopas yrityksille - ICC Cyber security guide for business*. ICC_CSG_PR.pdf (kauppakamari.fi)

Iivari, M., Laaksonen, M. (2009). *Liiketoiminnan jatkuvuussuunnittelu ja ICT -varautuminen*. Tietosanoma. Helsinki.

International Energy Agency IEA (2024). *Electricity 2024 – Analysis and forecast to 2026*. International Energy Agency. Electricity 2024 - Analysis and forecast to 2026

ISMS (ei pvm.). ISO/IEC 27000. isms.online. https://www.isms.online/iso-27000/

Jovanovic, B. (2024). *Internet of Things statistics for 2024 – Taking Things Apart*. DataProt verkkoartikkeli 6.2.2024. Saatavilla 21.11.2024. Internet of Things statistics for 2024 - Taking Things Apart

Juhila, K. (2021). *Teemoittelu*. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Saatavilla 22.11.2024. Teemoittelu - Tietoarkisto (tuni.fi)

June, C. (2015). *Michigan Micro Mote (M3) makes history´s smallest computer*. Michiganin yliopisto ECE (Electrical Computer Engineering 18.3.2015. https://ece.engin.umich.edu/stories/michigan-micro-mote-m3-makes-history-as-the-worlds-smallest-computer

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

Khaldi, A., Daniel, E., Massin, L., Kärnfelt, C., Ferranti, F., Lahuec, C., Seguin, F., Nourrit, V. & de Bougrenet de la Tocnaye, J.-L. (2020). *A laser emitting contact lens for eye tracking*. Scientific Reports 10, artikkeli 14804, 2020. https://doi.org/10.1038/s41598-020-71233-1

Kim, J., Kim, M., Lee, M.-S., Kim, K., Ji, S., Kim, J.-T., Park, J., Na, K., Bae, K.-H., Kim, H., Bien, F. Lee, C. & Park, J.-U. (2017). *Wearable smart sensor systems integrated on soft contact lenses for wireless ocular diagnostics*. Nature Communications 8, artikkeli 14997, 2017. https://doi.org/10.1038/ncomms14997

Kirtley, N. (2024) *EU NIS2, DORA, CRA and AI Act*. verkkoartikkeli 22.10.2024. Saatavilla 21.11.2024. EU NIS2, DORA, CRA and AI Act - Threat-Modeling.com

Kyberturvallisuuskeskus (2020). *Kyberturvallisuus ja yrityksen hallituksen vastuu*. Traficomin julkaisu 2/2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskus (2023a). *Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa - ohje johdolle ja asiantuntijoille*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje

Kyberturvallisuuskeskus (2023b). *Ohjeet ja oppaat organisaatioille ja yrityksille*. Tietoturvaohjeita yrityksille | Kyberturvallisuuskeskus.

Kyberturvallisuuskeskus (2024). Ajankohtaista. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset?limit=20&offset=0&query=&sort=updated

Laskurix (2024). *Keskiarvo-, moodi-, ja mediaanilaskuri*. Saatavilla 22.11.2024. Keskiarvo-, moodi-, ja mediaanilaskuri – Laskurix

Latvala, O-M. (2022). *Policy brief – kvanttiturvalliset salausmenetelmät Suomessa*. VTT:n julkaisu 2022. Kvanttiturvalliset salausmenetelmät Suomessa

Lehto, M. (2023). *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto.

Likert, R. (1932). *A Technique for the Measurement of Attitudes*. Archives of Psychology, 140, 5-53. New York University.

Loihde (11.3.2024). *Vastuu NIS2 -direktiivin noudattamisesta on yritysten johdolla*. https://www.loihdetrust.com/blogi/vastuu-nis2-direktiivin-noudattamisesta-on-yritysten-johdolla/

Microsoft (2023). *Evolving Zero Trust*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Microsoft (2024). *Microsoft Digital Defense Report 2024*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Neittaanmäki, P., Lehto, M., Savonen, M. (2021). Yhteiskunnan Digimurros. https://jyx.jyu.fi/bitstream/handle/123456789/75328/Yhteiskunnan%20digimurros.pdf?sequence=1&isAllowed=y

Neuralink (2024). *Etusivu*. Saatavilla 21.11.2024. https://neuralink.com/

Nikhat, A., & Yusuf, P. (2020). *The internet of nano things (IoNT) existing state and future Prospects*. GSC Advanced Research and Reviews, *5*(2), 131–150. https://doi.org/10.30574/gscarr.2020.5.2.0110

National Institute of Standards and Technology NIST (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (NIST SP 800-160 Vol. 2 Rev. 1). Developing Cyber-Resilient Systems; A Systems Security Engineering Approach (nist.gov).

Open Web Application Security Project OWASP (2023). *Etusivu*. Saatavilla 21.11.2024. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation

Pathak, V., Pandya, R.J., Bhatia, V., Lopez, O.A. (2023). *Qualitative Survey on Artificial Intelligence Integrated Blockchain Approach for 6G and Beyond*. IEEE Access 11, s. 105935-105981, 2023. doi:10.1109/ACCESS.2023.3319083

Porambage, P., Gür, G., Osorio, D., Liyanage, M., Ylianttila, M. (2021). *6G Security Challenges and Potential Solutions*. 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCN/6G) verkkokonferenssi 8.-11.6.2021. Saatavilla 21.11.2024 nbnfi-fe2021081643336.pdf

Rouse, M. (2024). *Tekoäly AI*. Techopedia Sanasto. 3.9.2024. Saatavilla 20.11..2024. https://www.techopedia.com/fi/sanasto/tekoaly-ai

Rousku, K. (2017). *Ohje Riskienhallintaan*. Valtiovarainministeriön julkaisuja 22/2017. Julkisen hallinnon ICT. Helsinki 2017. Ohje riskienhallintaan (valtioneuvosto.fi)

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *Aineisto- ja teorialähtöisyys*. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Saatavilla 22.11.2024. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_3_2_3.html

Sanastokeskus (2004). *Terminologiset sanastot – haktivisti*. TSK 31, 2004. haktivisti | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

Sanastokeskus (2010). *terminologiset sanastot 2 – IT, ICT*. Tietotekniikan termitalkoot 5.3.2010. https://termipankki.fi/tepa/fi/haku/ict

Sanastokeskus (2013). *Terminologiset sanastot 2 – massadata*. Tietotekniikan termitalkoot 16.12.2013. massadata | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

Sanastokeskus (2014). *Terminologiset sanastot 2 – palvelunestohyökkäys*. Tietotekniikan termitalkoot 5.12.2014. https://termipankki.fi/tepa/fi/haku/palvelunestohy%C3%B6kk%C3%A4ys

Sanastokeskus (2016a). *Terminologiset sanastot 2 – jatkuvuussuunnitelma*. Tietotekniikan termitalkoot 11.7.2016 https://termipankki.fi/tepa/fi/haku/jatkuvuussuunnitelma

Sanastokeskus (2016). *Terminologiset sanastot 2 – toipumissuunnitelma*. Tietotekniikan termitalkoot 11.7.2016. https://termipankki.fi/tepa/fi/haku/toipumissuunnitelma

Sanastokeskus (2017). *Terminologiset sanastot 2 – IoT*. Tietotekniikan termitalkoot 24.2.2017. https://termipankki.fi/tepa/fi/haku/iot

Sanastokeskus (2018a). *Kyberturvallisuuden sanasto - jatkuvuudenhallinta*. Kyberturvallisuuden sanasto TSK 52, 2018). https://termipankki.fi/tepa/fi/haku/jatkuvuudenhallinta

Sanastokeskus (2018b). *Terminologiset sanastot 2 – lohkoketju*. Tietotekniikan termitalkoot 18.4.2018. lohkoketju | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

Sanastokeskus (2018b). *Terminologiset sanastot 2 – nollapäivähaavoittuvuus*. Tietotekniikan termitalkoot 26.8.2018. nollapäivähaavoittuvuus | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

Sanastokeskus (2018c). *Terminologiset sanastot – tietoturvaloukkaus*. Kyberturvallisuuden sanasto TSK 52, 2018. https://termipankki.fi/tepa/fi/haku/tietoturvaloukkaus

Sanastokeskus (2022). *Terminologiset sanastot 2 – tekoäly*. Tietotekniikan termitalkoot 24.1.2022. tekoäly | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

Schneider, J. & Smalley, I. (2024). *What is quantum computing?*. IBM verkkoartikkeli 5.8.2024. Saatavilla 21.11.2024. What Is Quantum Computing? | IBM

Sengar, S., Hasan, A., Kumar, S., & Carroll, F. (2024). *Generative Artificial Intelligence: A Systematic Review and Applications*. ArXiv, abs/2405.11029. https://doi.org/10.48550/arXiv.2405.11029

SFS Suomen Standardit (ei pvm.). *Mitä standardi tarkoittaa?* https://sfs.fi/standardeista/mika-on-standardi/

SFS-EN 9001:2015 (2015). *Laadunhallintajärjestelmä. Vaatimukset*. SFS-EN ISO 9001

SFS-EN ISO 22301:2019 (2019). *Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset*. SFS-EN ISO 22301:2019

SFS-EN ISO/IEC 27001:2022 (2022). *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.* *SFS-EN ISO/IEC 27002:2022*

SFS-EN ISO/IEC 27001:2023 (2023). *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset*. SFS-EN ISO/IEC 27001:2023

SFS-ISO 31000:2018 (2018). *SFS-ISO 31000:2018 Riskienhallinta. Ohjeet.* SFS-ISO 31000:2018

Spedan (21.4.2019). 5 Business Continuity terms you must know. https://spedan.co.uk/blog/iso-22301-business-continuity/5-business-continuity-terms-you-must-know

Taherdoost, H. (2022a). *Cybersecurity vs. Information Security*. Procedia Computer Science 215. Joulukuu 2022, s. 483.487. https://doi.org/10.1016/j.procs.2022.12.050

Taherdoost, H. (2022b). *Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview*. Electronics 2022, 11(14). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview.

Tilastokeskus (2024). Keskiluvut. Saatavilla 22.11.2024. Keskiluvut | Käsitteet | Tilastokeskus

Traficom (2020). *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)*. PiTuKri – versio 1.1 – maaliskuu 2020. Traficomin julkaisu 13/2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Tuomi, J., Sarajärvi, A. (2018) *Laadullinen tutkimus ja sisällönanalyysi* (uud. laitos). Helsinki: Tammi.

Turvallisuuskomitea (2018). *Kyberturvallisuuden sanasto (TSK 52)*. Helsinki: Sanastokeskus TSK Ry. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Valtiovarainministeriö (ei pvm.). *Riskienhallinta*. Saatavilla 21.11.2024. Riskienhallinta - Valtiovarainministeriö

Valtiovarainministeriö (2012). *ICT -varautumisen vaatimukset*. VAHTI 2/2012. Valtionhallinnon tietoturvallisuuden johtoryhmä. https://vm.fi/documents/10623/307669/ICT-varautumisen+vaatimukset/9fa21bee-efcc-485a-8677-4eb4e0a2fa1f/ICT-varautumisen+vaatimukset.pdf

Valtiovarainministeriö (2016a). *Toiminnan jatkuvuuden hallinta*. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – Vahti -ohje 2/2016.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75168/VAHTI_2_2016.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö (2016b). *Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi*. OECD:n suositus ja liiteasiakirja. Valtiovarainministeriön julkaisu 28/2016. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75412/OECD_julkaisu_NETTI.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö (2023). *Julkisen hallinnon tietoturvallisuuden auditointikriteeristö (Julkri)*. Valtiovarainministeriön julkaisu 2023:46. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165015/VM_2023_46_Julkri.pdf?sequence=1&isAllowed=y

Valtioneuvoston kanslia (2024). Suomen kyberturvallisuusstrategia 2024-2035. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1&isAllowed=y

World Economic Forum WEF (2024). *Global Cybersecurity Outlook 2024 – Insight Report January 2024*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Yassine, M. (2021). *IT/OT convergence and cybersecurity*. Computer Fraud and Security, joulukuu 2021, 13-16. (PDF) IT/OT convergence and cybersecurity.

Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., & Oppermann I., (Eds.). (2020). *6G White Paper: Research Challenges For Trust, Security And Privacy*. 6G Research Visions, Numero 9. Oulun yliopisto. https://urn.fi/URN:ISBN:9789526226804

LIITE 1 KYSELYTUTKIMUKSEN ESITTELYTEKSTI

Kyselytutkimus on osa aineistonkeruuta Kyberturvallisuuden maisteritutkinnon pro-gradu -tutkielmaan aiheesta "Kyberturvallisuuden tehokkaampi hyödyntäminen organisaatioiden jatkuvuudenhallinnassa nyt ja huomenna". Tutkielman tavoitteena on selvittää miten hyvin kyberturvallisuus ja sen keinot on huomioitu organisaatioissa kokonaisuudessaan osana jatkuvuudenhallintaa, miten hyvin organisaatioiden koetaan olevan varautuneita nykyisiin ja nouseviin kyberuhkiin jotka voivat vaarantaa niiden toiminnan jatkuvuuden, sekä miten varautumista tällä puolella voitaisiin tehostaa. Kyselyn tavoitteena on saada kuva aihealueen parissa työskentelevien asiantuntijoiden ja ammattilaisten puolelta avuksi nykytilanteen hahmottamisessa, sekä tehostamisehdotusten kartoittamisessa proaktiivisesti.

Kysely on kohdistettu henkilöille joilla on suoraan tai välillisesti kokemusta, tietoa ja ymmärrystä organisaatioiden jatkuvuudenhallinnasta ja sen keinoista, sekä kyberturvallisuudesta osana jatkuvuudenhallintaa. Vastaukset pyydetään antamaan kokonaiskuvana sen käsityksen ja tietojen mukaan mitä vastaajalle on muodostunut työn, koulutuksen, ja / tai kokemuksen kautta, eikä kyselyssä pyydetä täsmentämään koskevatko vastaukset yhtä vai useampaa organisaatiota, tai alan kokonaiskuvaa aihealueen sensitiivisyyden vuoksi.

Kyselyn osalta tiedostetaan, että varautuminen esim. suurien tai kriittiseen infrastruktuuriin liittyvien organisaatioiden, sekä pienten-keskisuurien (p-k) yritysten välillä eroaa toisistaan. Tästä syystä kyselyn alussa pyydetään valitsemaan kohdistuvatko vastaukset pieniin ja keskisuuriin organisaatioihin, vai suuriin tai kriittiseen infrastruktuuriin kuuluviin organisaatioihin. Kriittisiä organisaatioita ei eritellä omaksi ryhmäkseen kyselyn anonymiteetista huolimatta. Jos vastaajalla on mahdollisuus sekä käsitystä molempiin kategorioihin liittyvien organisaatioiden varautumisesta aihealueeseen liittyen on kyselyyn mahdollista vastata useamman kerran.

Kyselyyn vastataan anonyymisti, eikä mitään vastaajien henkilöiviä tietoja tallenneta järjestelmään (Webropol). Kyselyn tulokset ovat nähtävissä kyselyn tekijälle, sekä Webropolin ylläpitäjille. Kyselyn tuloksia säilytetään järjestelmän määritysten mukaisesti. Kyselyyn vastaaminen on vapaaehtoista ja sen voi keskeyttää missä vaiheessa tahansa. Kysely on ainoastaan pro-gradu -tutkielmaa varten eikä vastaamisesta saa palkkiota.

Kysely koostuu kolmesta (3) aihealueesta (valmistautuminen ja suunnittelu, valmiudet, sekä metodit ja työkalut) jotka sisältävät 5-8 monivalintakysymystä /-väittämää per osio. (Yhteensä 19). 4. osio koostuu vapaaehtoisista avoimista kysymyksistä joilla vastaaja voi halutessaan täydentää vastauksiaan ja antaa lisätietoa tutkimuksen aihealueeseen liittyen. Kyselyn monivalintaosioon vastaaminen vie n. 10-15 minuuttia.

Kysely on voimassa 2.10-7.11.2024

LIITE 2 KYSYMYSPATTERISTO

	Kyselyn kysymykset
1.	**Tämän osion kysymykset kohdistuvat organisaatioiden jatkuvuudenhallintaan liittyvään valmistautumiseen ja suunnitteluun keskittyen kyberturvallisuuteen.**
1.	Kuinka hyvin koette organisaatioiden tunnistaneen näiden kriittiset suojattavat toiminnot, omaisuuden (assets) ja resurssit?
2.	Kuinka hyvin kyberturvallisuus ja sen keinot on mielestänne huomioitu kokonaisuudessaan osana organisaatioiden jatkuvuudenhallintaa?
3.	Kuinka hyvin koette organisaatioiden tunnistaneen kyberturvallisuusriskit jotka voivat uhata liiketoiminnan jatkuvuutta?
4.	Kuinka hyvin koette organisaatioiden varanneen riittävät henkilöresurssit ja budjetin kyberturvallisuudesta huolehtimiseen osana jatkuvuudenhallintaansa?
5.	Kuinka hyvin koette organisaatioiden huomioineen toimitus- ja alihankintaketjujen aiheuttamat riskit jatkuvuudenhallinnassa kyberturvallisuuden kannalta?
6.	Kuinka hyvin koette organisaatioiden tunnistavan nousevat ja uudet jatkuvuuteen vaikuttavat kyberuhat ja varautuvan niiltä suojautumiseen ennakoivasti suunnittelussaan?
2.	**Tämän osion väittämät käsittelevät organisaatioiden koettua valmiutta vastata vakaviin jatkuvuuteen vaikuttaviin kyberuhkiin, -poikkeamiin ja -hyökkäyksiin.**
7.	Organisaatioiden kyberturvallisuuspolitiikka ja muun aihealuetta ohjaava dokumentaatio, sekä toipumis- ja jatkuvuussuunnitelmat tukevat jatkuvuudenhallintaa riittävällä tasolla:
8.	Organisaatiot pystyvät palautumaan vakavista jatkuvuuteen vaikuttavista kyberhyökkäyksistä ilman merkittäviä vaikutuksia niiden toiminnoille:
9.	Organisaatiot pystyvät reagoimaan kyberhyökkäyksiin riittävän nopeasti siten, että niillä ei ole merkittävää vaikutusta kriittisiin toimintoihin:
10.	Organisaatiot ovat varautuneet toimitus- ja hankintaketjujen kautta organisaatioon kohdistuviin jatkuvuuteen vaikuttaviin hyökkäyksiin ja riskeihin riittävällä tasolla:
11.	Organisaatioiden valmiudet vastata uusiin ja nouseviin kyberuhkiin ovat riittävällä tasolla:
12.	Organisaatioilla on käytössään nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin nähden ajantasaiset prosessit ja ohjeistukset joita päivitetään säännöllisesti uhkakuvien mukaisesti.
3.	**Tämän osion väittämät käsittelevät organisaatioiden kyberturvallisuuteen kohdistettuja metodeja, prosesseja ja työkaluja.**
13.	Organisaatioiden kyberturvallisuustoimenpiteet ovat kokonaisuutena tarkastellen riittävät suojaamaan organisaatiota uusimmilta uhkilta ja haavoittuvuuksilta.
14.	Organisaatioilla on käytössään riittävät tekniset keinot, valmiudet ja työkalut vastata nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin.
15.	Organisaatiot suorittavat harjoituksia ja testaavat kyberturvallisuuttaan riittävästi huolehtiakseen kriittisten resurssiensa suojaamisesta.
16.	Testauksissa ja harjoituksissa huomioidaan tämän hetken merkittävimmät, sekä nousevat organisaatioihin kohdistuvat kyberuhat.
17.	Organisaatioiden kriisi- poikkeustilanneviestintä kyberturvallisuuspoikkeamiin liittyen on riittävän tehokasta ja saavuttaa kaikki tarvittavat osapuolet riittävällä tasolla.
18.	Organisaatiot tarjoavat riittävästi säännöllistä koulutusta työntekijöilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan jatkuvuudenhallinnassa.
19.	Organisaatiot tarjoavat riittävästi säännöllistä koulutusta toimittajilleen ja alihankkijoilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan organisaation jatkuvuudenhallinnassa.
4.	**Tässä osiossa on avoimia kysymyksiä joilla tarkennetaan aikaisempiin osioihin liittyviä aihealueita. Vastaaminen on vapaaehtoista, mutta auttaa tutkimuksen aihealueiden käsittelyn ja tutkimuksen syventämisessä**
21.	Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta?
22.	Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne.
23.	Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan?
24.	Vapaa sana. Voitte laittaa tähän ajatuksianne ja palautetta kyselyn aihealueeseen ja tutkimusaiheeseen liittyen.

LIITE 3 HAASTATTELUKYSYMYKSET

Haastattelun rakenne ja haastattelukysymykset

Alussa käydään läpi esittelyt. Tästä voi halutessaan kieltäytyä. Toivottaessa graduun ei laiteta mitään henkilön tunnistamiseen liittyviä tietoja (nimi, ammatti/positio), vaan nämä jätetään vain taustamateriaaleihin.

Haastattelun voi lopettaa missä vaiheessa tahansa, tai kieltäytyä vastaamasta kysymykseen (pääkysymykset toimitetaan ennakkoon, mutta keskustelun aikana voi tulla tarkentavia kysymyksiä aihealueeseen liittyen). Jos koet, että jokin tietty kysymys ei kohdistu omaan osaamisalaasi voi sen pyytää ohittamaan. Kysymykset ovat samat useammalle haastateltavalle vertailtavuuden vuoksi.

Mitkään kysymykset eivät liity suoraan mihinkään organisaatioon, vaan tutkimusaihetta käsitellään yleisemmällä tasolla.

Haastattelu nauhoitetaan litterointia varten, jos haastateltava hyväksyy tämän. Muussa tapauksessa haastattelija kerää muistiinpanot.

Haastattelunauhoitusta säilytetään niin kauan, kuin gradun kannalta on tarpeellista, tämän jälkeen nauhoite tuhotaan. Mahdollinen litterointi säilytetään muun gradunmateriaalin kanssa.

Kysymykset:

-Mikä on erikoistumisalanne? (Tällä tarkoitetaan haastateltavan ammatillista tai koulutuksellista osaamista, sekä erikoistumista alan sisällä).

-Kuinka hyvin kyberturvallisuus on otettu mielestänne otettu huomioon organisaatioiden jatkuvuudenhallinnassa nykyisin?

-Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta? (Kyselyn avoin kysymys)

-Jos organisaatio joutuu priorisoimaan toimenpiteitään suojatakseen jatkuvuuttaan, niin mitkä keinot näiden tulisi ensisijaisesti huomioida?

-Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne. (Kyselyn avoin kysymys)

-Mitkä ovat mielestänne merkittävimpiä nousevia teknologioita ja niiden aiheuttamia uhkia organisaatioiden jatkuvuuden kannalta nyt ja tulevaisuudessa?

-Mitkä näette merkittävimmiksi uhkiksi ja mahdollisuuksiksi organisaatioiden kyberturvallisuuden ja jatkuvuudenhallinnan kannalta erikoistumisalaanne nähden?

-Mitkä ovat kvanttiteknologian merkittävimmät uhat ja mahdollisuudet organisaatioille nyt ja tulevaisuudessa?

- Mitkä ovat 6G:n aiheuttamat merkittävimmät uhat ja mahdollisuudet organisaatioille nyt ja tulevaisuudessa?

-Näettekö nanoteknologian aiheuttavan uhkia nyt tai tulevaisuudessa? Jos, niin mitkä ovat merkittävimmät sen aiheuttamat uhat?

-Mitkä muut kehittyvät teknologiat ja trendit voivat uhata organisaatioiden jatkuvuudenhallintaa?

-Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan? (Kyselyn avoin kysymys)

-Miten vastaisitte tutkimuksen otsikon aiheeseen kysymysmuodossa: Miten näkisitte, että kyberturvallisuutta voitaisiin tehokkaimmin hyödyntää organisaatioiden jatkuvuudenhallinnassa nyt ja tulevaisuudessa?

Vapaa sana ja avointa keskustelua aihealueesta tai haastatteluun liittyen.
Nauhoitus päätetään (jos nauhoittaminen hyväksytty)

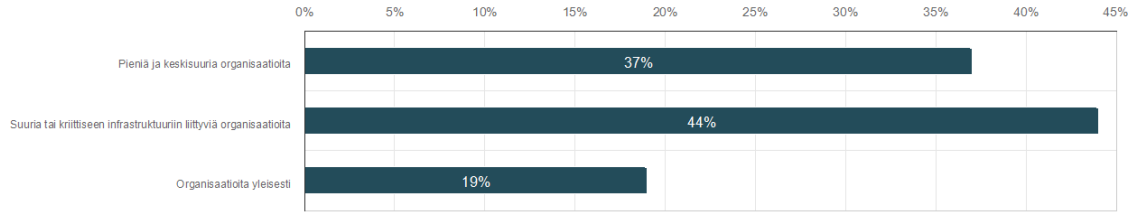
LIITE 4 KYSELYRAPORTTI

Perusraportti
Kyberturvallisuus osana organisaatioiden jatkuvuudenhallintaa

Vastaajien kokonaismäärä: 27

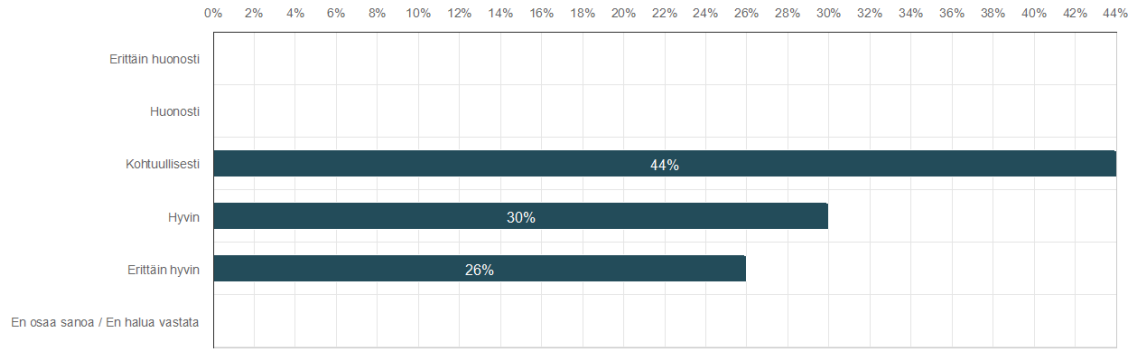
8 Käsittelevätkö vastaukset**:**

Vastaajien määrä: 27



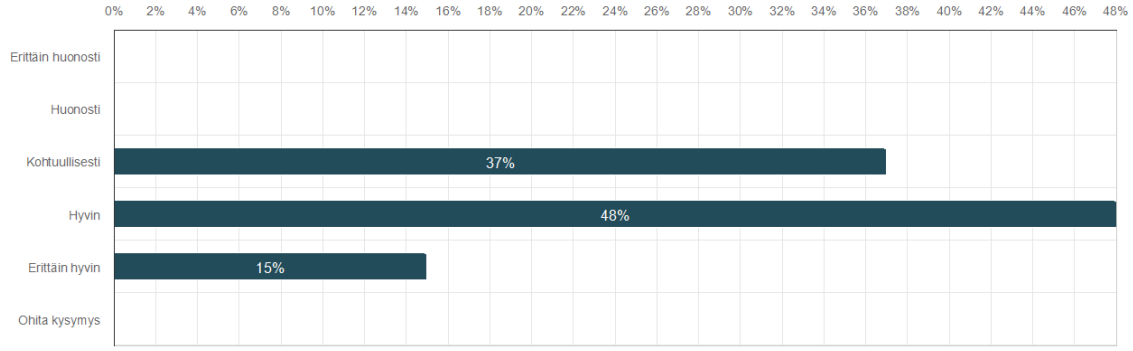
	n	Prosentti
Pieniä ja keskisuuria organisaatioita	10	37,0%
Suuria tai kriittiseen infrastruktuuriin liittyviä organisaatioita	12	44,5%
Organisaatioita yleisesti	5	18,5%

Kuinka hyvin koette organisaatioiden tunnistaneen näiden kriittiset suojattavat toiminnot, omaisuuden (assets) ja resurssit?
Vastaajien määrä: 27



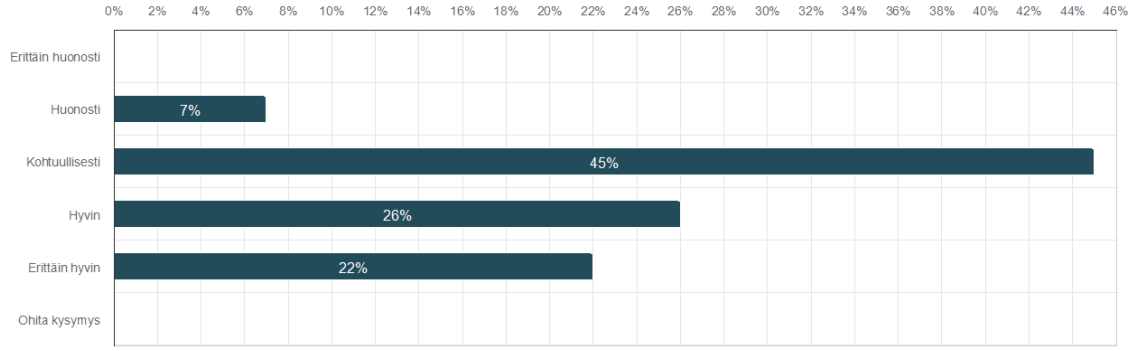
	n	Prosentti
Erittäin huonosti	0	0,0%
Huonosti	0	0,0%
Kohtuullisesti	12	44,5%
Hyvin	8	29,6%
Erittäin hyvin	7	25,9%
En osaa sanoa / En halua vastata	0	0,0%

Kuinka hyvin kyberturvallisuus ja sen keinot on mielestänne huomioitu kokonaisuudessaan osana organisaatioiden jatkuvuudenhallintaa?
Vastaajien määrä: 27



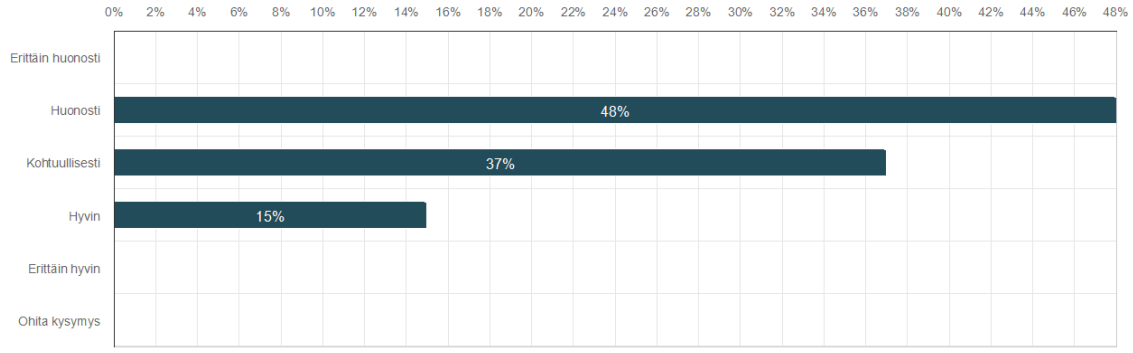
	n	Prosentti
Erittäin huonosti	0	0,0%
Huonosti	0	0,0%
Kohtuullisesti	10	37,0%
Hyvin	13	48,2%
Erittäin hyvin	4	14,8%
Ohita kysymys	0	0,0%

Kuinka hyvin koette organisaatioiden tunnistaneen kyberturvallisuusriskit jotka voivat uhata liiketoiminnan jatkuvuutta?
Vastaajien määrä: 27



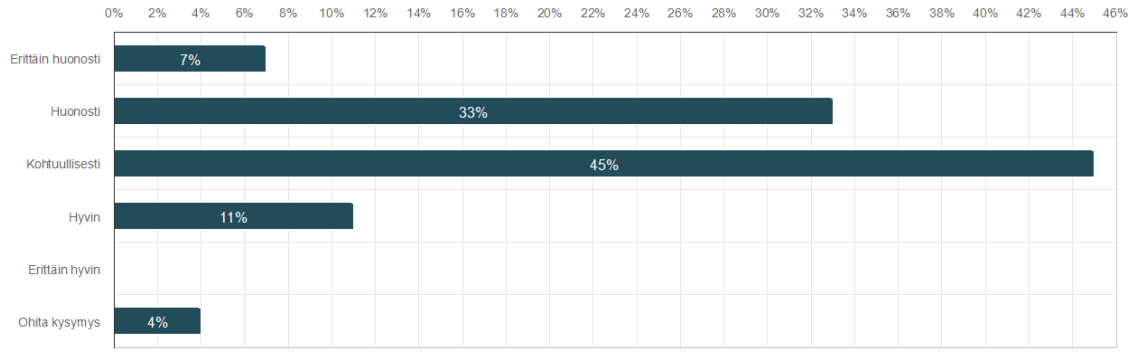
	n	Prosentti
Erittäin huonosti	0	0,0%
Huonosti	2	7,4%
Kohtuullisesti	12	44,5%
Hyvin	7	25,9%
Erittäin hyvin	6	22,2%
Ohita kysymys	0	0,0%

Kuinka hyvin koette organisaatioiden varanneen riittävät henkilöresurssit ja budjetin kyberturvallisuudesta huolehtimiseen osana jatkuvuudenhallintaansa?
Vastaajien määrä: 27



	n	Prosentti
Erittäin huonosti	0	0,0%
Huonosti	13	48,2%
Kohtuullisesti	10	37,0%
Hyvin	4	14,8%
Erittäin hyvin	0	0,0%
Ohita kysymys	0	0,0%

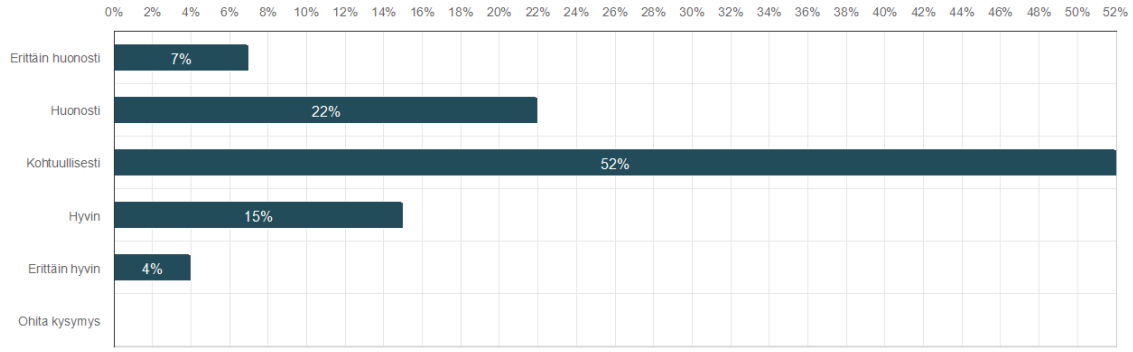
Kuinka hyvin koette organisaatioiden huomioineen toimitus- ja alihankintaketjujen aiheuttamat riskit jatkuvuudenhallinnassa kyberturvallisuuden kannalta?
Vastaajien määrä: 27



	n	Prosentti
Erittäin huonosti	2	7,4%
Huonosti	9	33,3%
Kohtuullisesti	12	44,5%
Hyvin	3	11,1%
Erittäin hyvin	0	0,0%

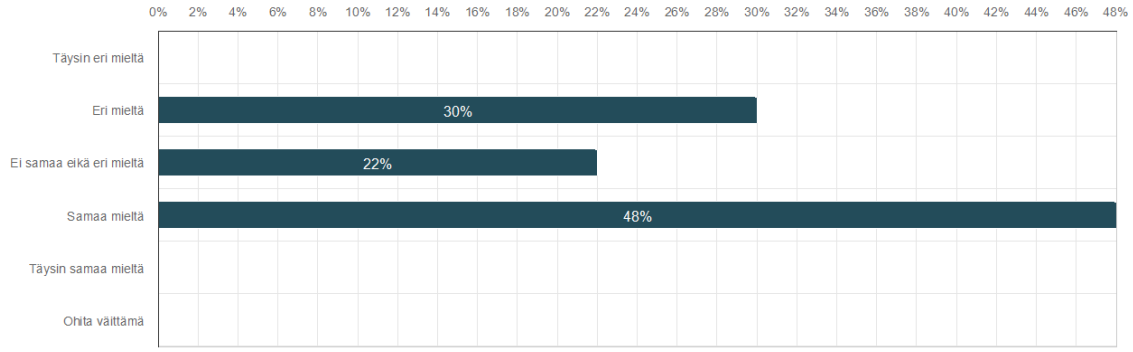
Ohita kysymys	1	3,7%

Kuinka hyvin koette organisaatioiden tunnistavan nousevat ja uudet jatkuvuuteen vaikuttavat kyberuhat ja varautuvan niiltä suojautumiseen ennakoivasti suunnittelussaan?
Vastaajien määrä: 27



	n	Prosentti
Erittäin huonosti	2	7,4%
Huonosti	6	22,2%
Kohtuullisesti	14	51,9%
Hyvin	4	14,8%
Erittäin hyvin	1	3,7%
Ohita kysymys	0	0,0%

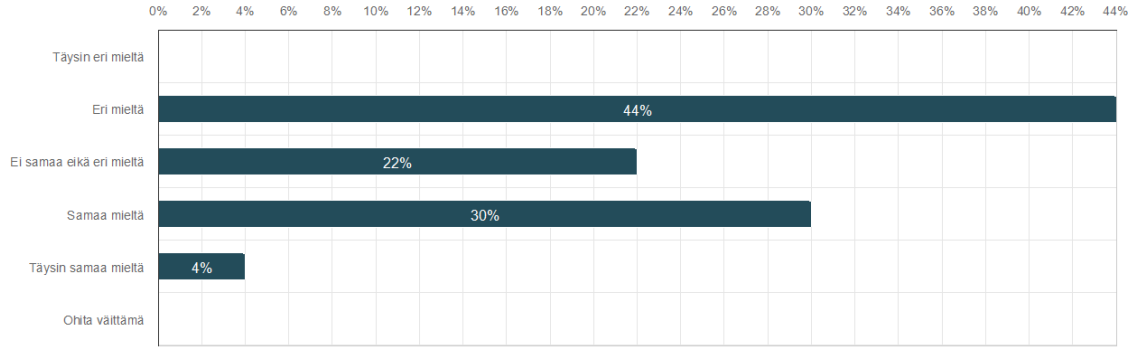
Organisaatioiden kyberturvallisuuspolitiikka ja muun aihealuetta ohjaava dokumentaatio, sekä toipumis- ja jatkuvuussuunnitelmat tukevat jatkuvuudenhallintaa riittävällä tasolla:
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	0	0,0%
Eri mieltä	8	29,6%
Ei samaa eikä eri mieltä	6	22,2%
Samaa mieltä	13	48,2%

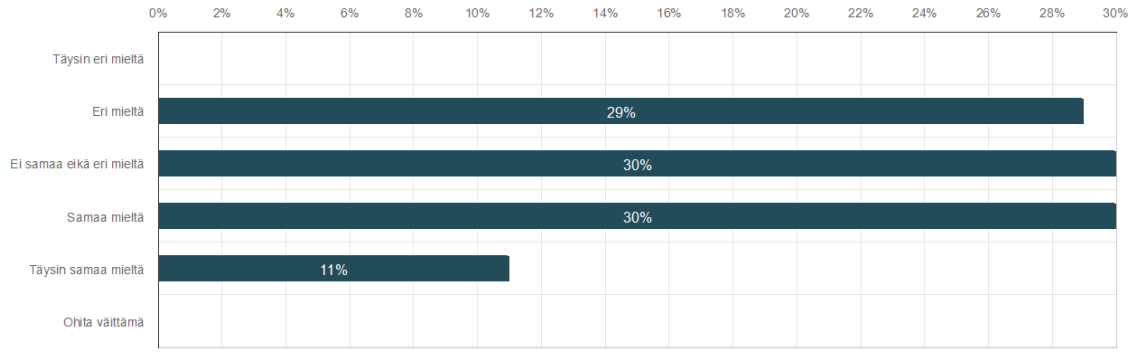
Täysin samaa mieltä	0	0,0%
Ohita väittämä	0	0,0%

Organisaatiot pystyvät palautumaan vakavista jatkuvuuteen vaikuttavista kyberhyökkäyksistä ilman merkittäviä vaikutuksia niiden toiminnoille:
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	0	0,0%
Eri mieltä	12	44,5%
Ei samaa eikä eri mieltä	6	22,2%
Samaa mieltä	8	29,6%
Täysin samaa mieltä	1	3,7%
Ohita väittämä	0	0,0%

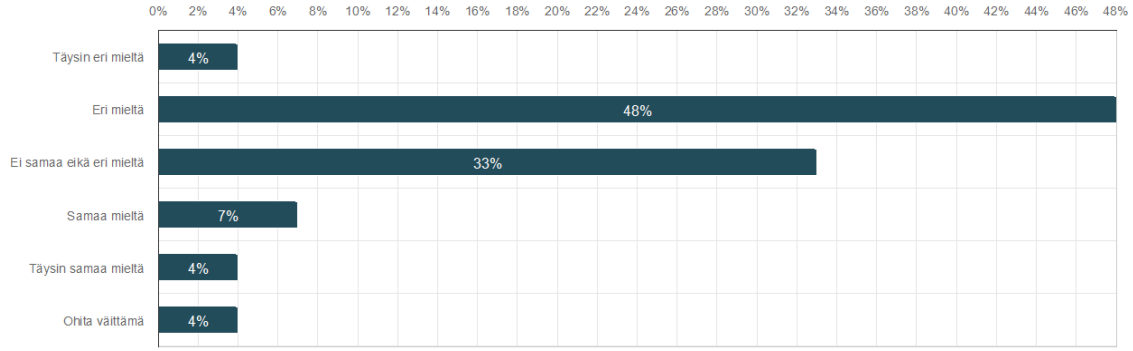
Organisaatiot pystyvät reagoimaan kyberhyökkäyksiin riittävän nopeasti siten, että niillä ei ole merkittävää vaikutusta kriittisiin toimintoihin:
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	0	0,0%
Eri mieltä	8	29,7%
Ei samaa eikä eri mieltä	8	29,6%

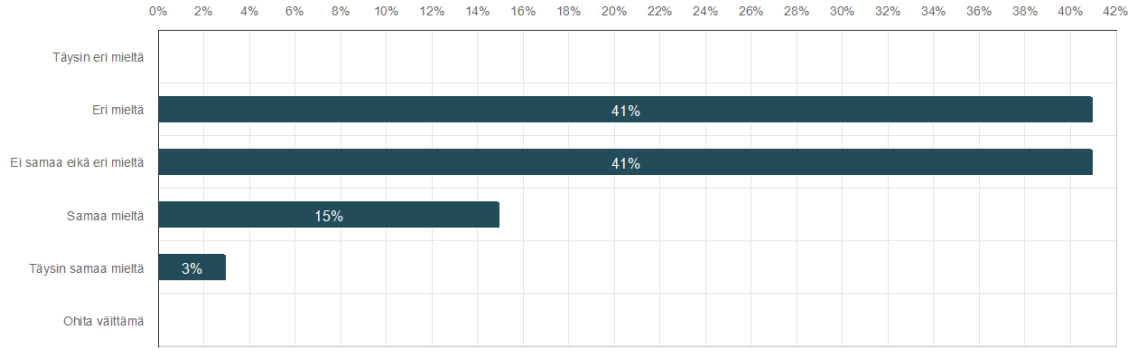
Samaa mieltä	8	29,6%
Täysin samaa mieltä	3	11,1%
Ohita väittämä	0	0,0%

Organisaatiot ovat varautuneet toimitus- ja hankintaketjujen kautta organisaatioon kohdistuviin jatkuvuuteen vaikuttaviin hyökkäyksiin ja riskeihin riittävällä tasolla:
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	13	48,2%
Ei samaa eikä eri mieltä	9	33,3%
Samaa mieltä	2	7,4%
Täysin samaa mieltä	1	3,7%
Ohita väittämä	1	3,7%

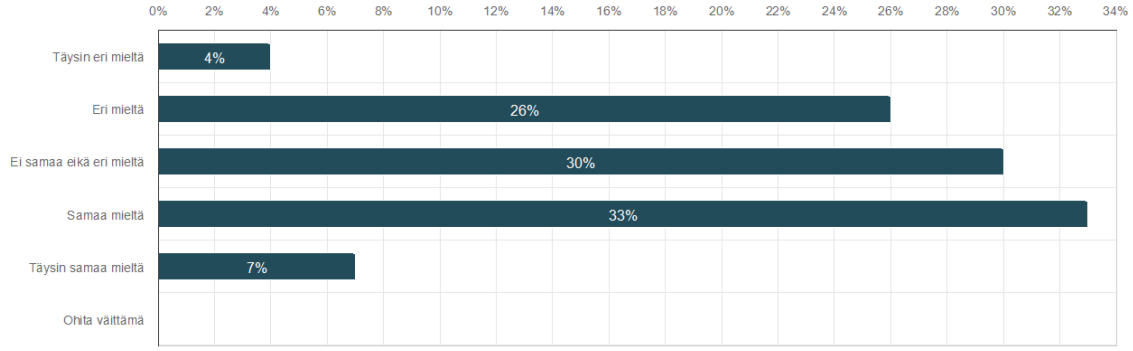
Organisaatioiden valmiudet vastata uusiin ja nouseviin kyberuhkiin ovat riittävällä tasolla:
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	0	0,0%
Eri mieltä	11	40,8%
Ei samaa eikä eri mieltä	11	40,7%

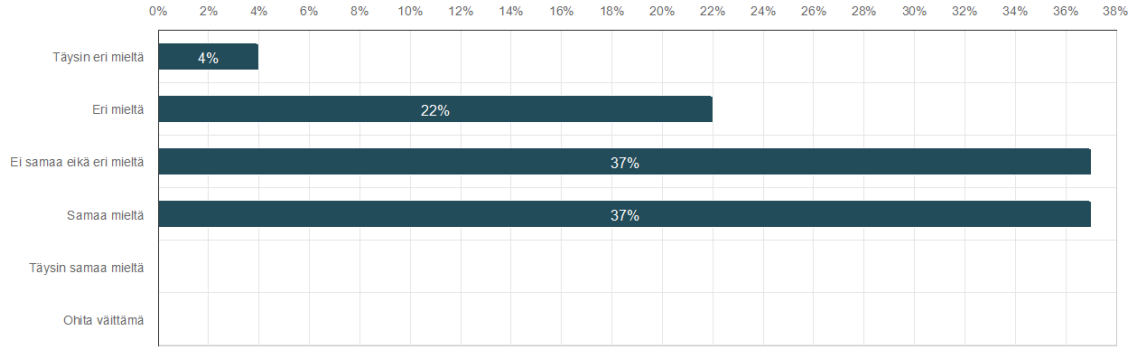
Samaa mieltä	4	14,8%
Täysin samaa mieltä	1	3,7%
Ohita väittämä	0	0,0%

Organisaatioilla on käytössään nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin nähden ajantasaiset prosessit ja ohjeistukset joita päivitetään säännöllisesti uhkakuvien mukaisesti.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	7	25,9%
Ei samaa eikä eri mieltä	8	29,6%
Samaa mieltä	9	33,4%
Täysin samaa mieltä	2	7,4%
Ohita väittämä	0	0,0%

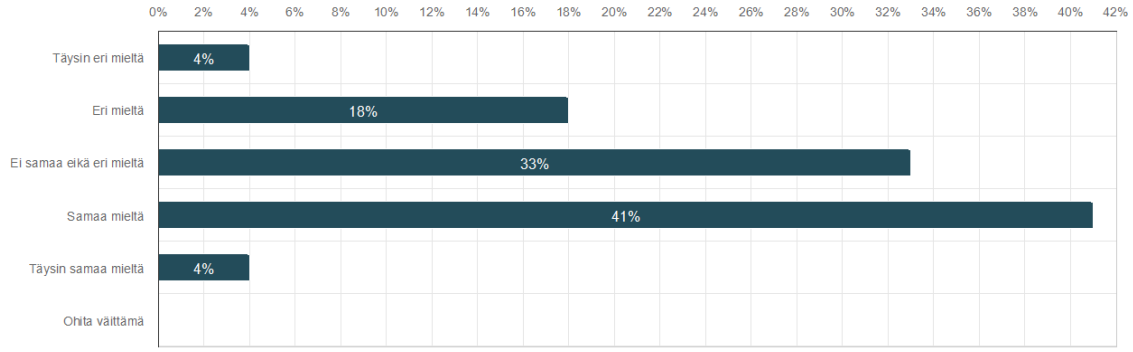
Organisaatioiden kyberturvallisuustoimenpiteet ovat kokonaisuutena tarkastellen riittävät suojaamaan organisaatiota uusimmilta uhkilta ja haavoittuvuuksilta.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	6	22,2%

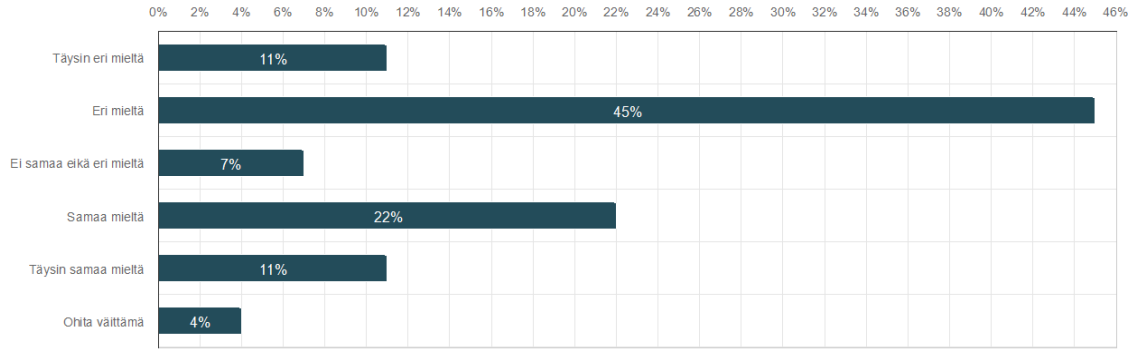
Ei samaa eikä eri mieltä	10	37,1%
Samaa mieltä	10	37,0%
Täysin samaa mieltä	0	0,0%
Ohita väittämä	0	0,0%

Organisaatioilla on käytössään riittävät tekniset keinot, valmiudet ja työkalut vastata nykyisiin ja nouseviin jatkuvuuteen vaikuttaviin kyberuhkiin.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	5	18,5%
Ei samaa eikä eri mieltä	9	33,3%
Samaa mieltä	11	40,8%
Täysin samaa mieltä	1	3,7%
Ohita väittämä	0	0,0%

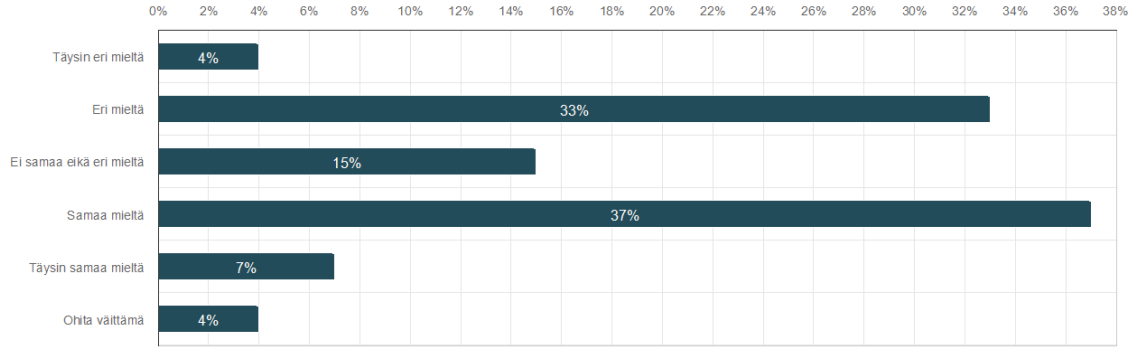
Organisaatiot suorittavat harjoituksia ja testaavat kyberturvallisuuttaan riittävästi huolehtiakseen kriittisten resurssiensa suojaamisesta.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	3	11,1%

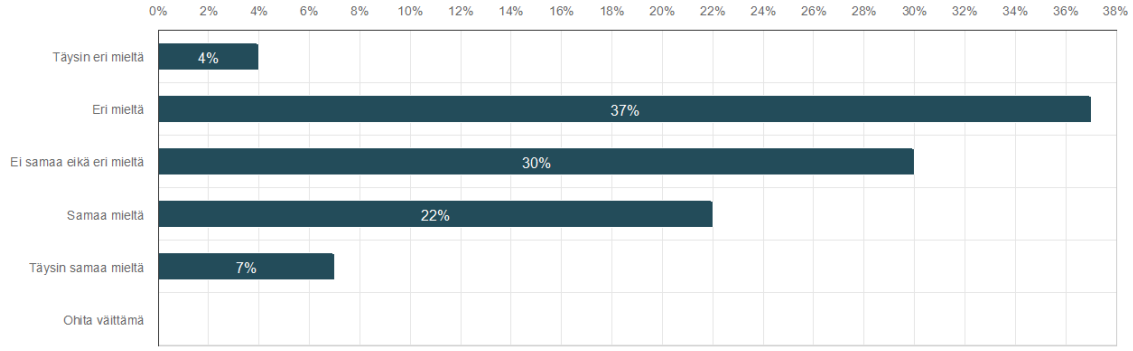
Eri mieltä	12	44,5%
Ei samaa eikä eri mieltä	2	7,4%
Samaa mieltä	6	22,2%
Täysin samaa mieltä	3	11,1%
Ohita väittämä	1	3,7%

Testauksissa ja harjoituksissa huomioidaan tämän hetken merkittävimmät, sekä nousevat organisaatioihin kohdistuvat kyberuhat.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	9	33,3%
Ei samaa eikä eri mieltä	4	14,8%
Samaa mieltä	10	37,1%
Täysin samaa mieltä	2	7,4%
Ohita väittämä	1	3,7%

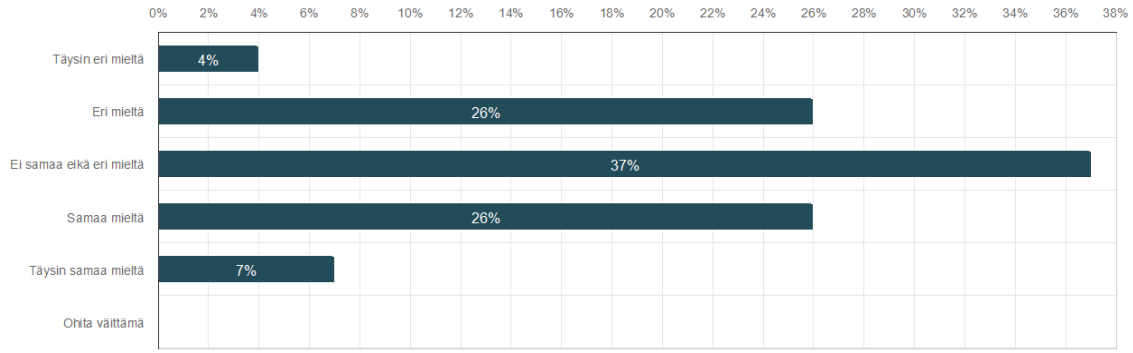
Organisaatioiden kriisi- poikkeustilanneviestintä kyberturvallisuuspoikkeamiin liittyen on riittävän tehokasta ja saavuttaa kaikki tarvittavat osapuolet riittävällä tasolla.
Vastaajien määrä: 27



	n	Prosentti

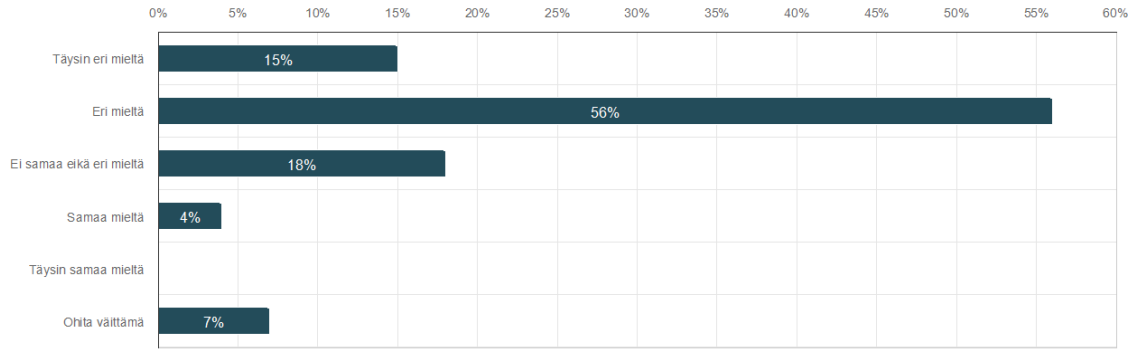
Täysin eri mieltä	1	3,7%
Eri mieltä	10	37,1%
Ei samaa eikä eri mieltä	8	29,6%
Samaa mieltä	6	22,2%
Täysin samaa mieltä	2	7,4%
Ohita väittämä	0	0,0%

Organisaatiot tarjoavat riittävästi säännöllistä koulutusta työntekijöilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan jatkuvuudenhallinnassa.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	1	3,7%
Eri mieltä	7	25,9%
Ei samaa eikä eri mieltä	10	37,1%
Samaa mieltä	7	25,9%
Täysin samaa mieltä	2	7,4%
Ohita väittämä	0	0,0%

Organisaatiot tarjoavat riittävästi säännöllistä koulutusta toimittajilleen ja alihankkijoilleen kyberturvallisuuden parhaista käytännöistä ja heidän roolistaan organisaation jatkuvuudenhallinnassa.
Vastaajien määrä: 27



	n	Prosentti
Täysin eri mieltä	4	14,8%
Eri mieltä	15	55,6%
Ei samaa eikä eri mieltä	5	18,5%
Samaa mieltä	1	3,7%
Täysin samaa mieltä	0	0,0%
Ohita väittämä	2	7,4%

Mitä mielestänne organisaatioiden tulisi erityisesti ottaa huomioon kyberturvallisuuden osalta huolehtiessaan jatkuvuudenhallinnasta?
Vastaajien määrä: 15

Vastaukset
Eri tietojärjestelmien, verkkoyhteyksien ja ensisijaisten resurssien rajapinnat ja keskinäiset riippuvuudet. Varsinkin riippuvuuksien osalta tulee toteutuneissa katkoksissa, testeissä, harjoituksissa tai auditoinneissa yllätyksiä vastaan lähes aina.
Tulisi tunnistaa organisaation kriittiset resurssit ja varmistaa niiden käytettävyys jatkuvuudenhallinnan näkökulmasta. Usein näkee liian paljon koko organisaatioon vietyjä hallintakeinoja, jolloin resursseja käytetään myös organisaation kannalta vähemmän tärkeiden resurssien suojaamiseen.
Tunnista sisäiset ja ulkoiset riippuvuudet. Investoi turvallisuuteen, priorisoi analyysin perusteella; peruskontrollit, taseen suojaus merkittävimmiltä uhilta esim vakuuttamalla. Kehitä kumppaniverkoston riskienhallintaa.
Varmentamisen suojaaminen ja palautumisen testaaminen.
On hyvä huomioida niin ohjelmien kuin laitteiden päivitykset, että molemmat ovat ajantasalla, koska tietoturvan ylläpitäminen vaatii aina uusia hankintoja tietoturva-aukkojen paikkaamiseksi. On hyvä miettiä myös laitteiden suojaus/hallinta rakennuksissa esim. isot serverihuoneet. Jos tällainen tila kärsii esim. vesivahingosta, voi sillä olla pitkä seuraus toiminnan jatkuvuuteen.
Riskien tunnistaminen ja erityisesti suojattavat kohteet (assets). Oman näkemykseni mukaan erityisesti PK -sektorin yritykset eivät ymmärrä riittävällä tasolla kyberuhkien vaikutusta omaan toimintaan erityisesti jos oma ydintoiminta ei ole IT keskeistä.
Tietysti dokumentaation ajantasalla pysyminen ja säännölliset läpikäynnit aiheesta.
Back up plan tilanteisiin jotka normaalisti saattaisivat jopa kaataa yrityksen.
Riittävät resurssit ja osaaminen
Riittävät resurssit investoinneissa taloudellisesti ja ajankäytöllisesti
Riittävä resursointi, ja sopimustekniset järjestelyt ovat usein heikko lenkki puhuttaessa jatkuvuudenhallinnan kybernäkökulmista. Lisäksi, tieto- ja kyberturvallisuuskoulutus antaa harvoin kokonaiskuvaa siitä, miksi asiat ovat tärkeitä, miten oma toiminta vaikuttaa kokonaisuuteen, ja millainen uhkakenttä omaa organisaatiota kohtaa.
Harjoitukset, joilla todennetaan todelliset kyvykkyydet, ei pelkästään tabletop-harjoituksia. Teknisten kyvykkyyksien lisäksi johdon roolit ja vastuut. Alihankintaketju ja sen kyvykkyydet sekä vastuut.
Tämän tulee olla johdon jatkuvassa seurannassa.

Perus asiat. Ohjeistuksia löytyy kyllä, mutta monesti niitä ei ole otettu riittävällä tasolla käyttöön. Lisäksi koulutus! koko organisaatio on alasta riippumatta koulutettava tunnistamaan erilaisia hyökkäys metodeja ja niiltä suojautumista.
-

Mitkä kyberuhat näette suurimpina uhkina organisaatioille tulevaisuudessa? Antakaa 3-5 mielestänne merkittävintä uhkaa. Voitte myös avata uhkien merkitystä halutessanne.
Vastaajien määrä: 15

Vastaukset
Osaamisresurssien puute. Teknisten ympäristöjen edelleen monimutkaistuessa ja uhkien kehittyessä mm. rikollisten ja valtiollisten toimijoiden käyttäessä tekoälyä suojaavat tekniset ratkaisut päivittyvät, mutta näiden tekniikoiden hyödyntämistä osaavien henkilöresurssien riittävyys on koetuksella. Vanhentuva tekniikka. Taloudellisten resurssien pienentyessä laitteita ei päivitetä tai vaihdeta ajallaan, jolloin haavoittuvia komponentteja voi jäädä vihamielisten tahojen hyödynnettäviksi tai esim. yhteensopivuushäiriöiden lähteiksi. Tekoälyn hallitsematon käyttö tai väärä luottamus sen tuottamiin tuloksiin. Hype ja aidosti valtavat mahdollisuudet aiheuttavat hallitsemattoman ja riskeistä piittaamattoman tekoälyn käytön esim. ohjelmistokehityksessä tai kyberuhkien havainnoinnissa.
Tekoälyn kehitys - uudet kasvavat uhkakuvat ja tekoälyyn liittyvien uusien suojattavien kohteiden (esim kielimallit) tunnistaminen. Toimitusketjujen turvallisuus - ketjut jatkavat venymistään, jolloin riskit kasvavat entisestään Organisaatioiden resurssien polarisoituminen - osa organisaatioista ymmärtää resurssien tarpeen ja toisessa ääripäässä mennään aivan minimaalisilla resursseilla. Konsolidoitumisen sijaan resurssien määrässä tapahtuu entistäkin kovempaa polarisoitumista.
Toimitusketju, AI, venäjä / kolmas maailmansota
Ransomware, tietojen varastaminen, tietojen julkaisulla kiristäminen, tietojen tuhoaminen.
Erilaiset palvelunestohyökkäykset, jotka hankaloittavat viestimistä asiakkaille tai estävät palvelun tuottamisen normaalisti. Tietojen kalastelut, joissa ihmisen huolimattomuus voi vaarantaa esim. henkilötietojen leviämisen (asiakkaat) tai työntekijöiden tietojen leviämisen, jolloin tietojen kalastelu leviää laajemmin organisaatiossa. Myös dis- ja misinformaation jakaminen virallisten lähteiden kautta esim. organisaation etusivulla asiakkaille voi aiheuttaa väärän tiedon leviämisen ja suuren mainehaitan.
- Kiristyshaittaohjelmat / vastaavat toiminnan lamauttavat haittaohjelmat - Palvelunestohyökkäykset - Tietomurrot
Kalastelu on parantunut niin hyvin viimeaikoina, enää ei voi luottaa suomenkielen "turvaan". Toimitusketjun pettäminen, sovellushankintoja tehdessä pitäisi varmistaa tavalla tai toisella että kaikki tomittajat sitoutuvat järjestelmän ylläpitoon ja päivityksiin ym. Vanhoista järjestelmistä kiinni pitäminen, yleensä joku käyttäjä pitää viimeiseen asti kiinni jostain iänikuisesta legacy järjestelmästä jonka tieturva ja päivitykset ovat jo aikaa sitten menneet vanhoiksi. Ei haluta luopua "hyvin toimivasta" vaan kynsin ja hampain pidetään kiinni vaikka järkevintä olisi hommata joku uudenaikainen tilalle.
Entiteettivarkaus Disinformaatio Datamurto Datan hijacking
Tietojen kalastelu onnistuessaan avaa pääsyn verkkoon.

Vihamieliset valtiolliset toimijat yleisesti
Nopeasti kehittyvät uudet teknologiat, jotka laajentavat organisaatioiden hyökkäyspinta-alaa sekä niitä käyttöönotettaessa että kyberrikollisten käsissä. Reagointiajan merkittävä lyhentyminen haavoittuvuuksien hyödyntämisessä. Riskienhallinnan puutteet - kyberriskejä ei pitäisi arvioida (ja hallita) erillään muusta riskienhallinnasta, ja jokainen tunnistettu riski tulisi arvioida myös kyberturvallisuuden näkökulmasta. Jompikumpi, tai molemmat, yleensä puuttuvat.
Merkittävät palveluiden ongelmat vrt Azure, Crowdstrike, Cloudflare -ongelmat. Phishing ja sen kautta saadut pääsyt järjestelmiin. Vulnerability Management ja patch Management hitaus tai huono kattavuus.
Tiedonkalastelu Tietovuoto Valtiolliset hyökkäykset
yleisesti tulevaisuuden uhat. Uusia haavoittuvuuksia löytyy lähes päivittäin. Tästä syystä olisi tärkeää, että tehtäisiin mahdollisimman paljon Threat hunting sisäisesti. Nolla päivä haavoittuvuudet ovat iso riski. Käyttäjät ovat edelleen isoin riski ja siksi jatkuva koulutus!
Alihankinta ja toimitusketjut, avoimen lähdekoodin sovellukset ja modulit

Mitkä kyberturvallisuuden varmistamiseen tarkoitetut työkalut / metodit näette organisaatioille tärkeimpinä suojautumisessa jatkuvuuteen vaikuttavia kyberuhkia vastaan?
Vastaajien määrä: 15

Vastaukset
Aidot, mutta ei liian jähmeät liiketoiminnan vaikutusanalyysit (BIA) tietotekniseen infraan ja tietojärjestelmiin. BIA on jatkuvuudenhallinnan perustyökaluja, mutta sitä pitäisi hyödyntää myös kyberturvallisuuden näkökulmasta tunnistamaan erilaiset riippuvuudet ja ensisijaiset komponentit, joita suojata myös tietojen luottamuksellisuuden ja eheyden osalta. Mielestäni kyberturvallisuutta ja toiminnan jatkuvuudenhallintaa ei pitäisi käsitellä erillisinä kokonaisuuksina, vaan nähdä näiden olevan lähes kaikilla toimialoilla ja organisaatioissa samaa asiaa: tavoitteena turvata toiminnan jatkuvuus häiriöiden tyypistä tai aiheuttajasta riippumatta.
Tekoäly tulee tarjoamaan myös mahdollisuuksia suojautumiseen/jatkuvuuden hallintaan ja erityisesti organisaatioille parhaiten sopivien hallintakeinojen valintaan. Kriittistä on siis osaamisen kehittäminen ja ymmärryksen kasvattaminen riskienhallinnasta yleisesti.
Jatkuvuussuunnittelu, vikasietoisuus, harjoittelu sekä kybersuojan kehittäminen.
Henkilöstön koulutus on aina tärkeää, koska ei-asian parissa työskentelevät kaipaavat lisää tukea ja varmuutta tekemiseen. Ihminen on heikoin, mutta samalla myös vahvin lenkki monessa tapauksessa. Esim. osa voi sortua kalasteluyritykseen, kun toiset taas raportoivat epäillyttävän tiedon heti. Aktiivinen riskienhallinta niin tietoturvallisuuden kuin organisaation muiden osa-alueiden osalla. Kun on tunnistettu riskit ja mietitty niille hallintatoimenpiteet, on niihin helpompi varautua. Toki asiat pitää pitää säännöllisesti esillä esim. johtoryhmien kokouksissa. Erilaiset ohjelmisto- ja laitehankinnat, jotta tarvittavat päivitykset tietoturvallisuuteen saadaan ylläpidettyä. Tässä pitää muistaa organisaation tarpeet ja osaaminen, ei ole tarvetta hankkia joka vuosi uusimpia laitteita, mutta säännöllinen tarkastus tarpeille on hyvä tehdä. Näin voidaan suunnitella hankintoja pitemmillä aikaväleillä.
Koulutus sekä harjoittelu / simulaatiot mitkä osallistavat mahdollisimman suuren osan henkilöstöä.
- CSOC-palvelu, jonka avulla pystytään reagoimaan tietoturvatapahtumiin

- Tietoturvan testaaminen esim. haavaskannereilla tai penetraatiotestauksilla, ja näiden tulosten hyödyntäminen kehitystyössä, eli ei riitä että testataan, vaan puutteet pitää lähtökohtaisesti myös korjata. - Henkilöstön kouluttaminen, opastaminen ja käyttäytymisen ohjaaminen säännöllisesti ja monipuolisesti
Käyttäjien koulutus ylipäätään, oli kyse sitten uhkien tunnistamisesta, ilmoittamisesta tai mistä tahansa tietotekniikkaan liittyvästä. Kunnollinen dokumentaatio. Harjoittelu uhkia vastaan. Palautusharjoitukset kriittisiin järjestelmiin.
Nollatietsikat Palomuurit Päivitetyt reitittimet ja keskittimet Salasanapolitiikka
Riittävät ratkaisut ja ulkoistettu valvonta
koulutus
Päivityssykli. Toimitusketjut. Sopimukset. Riittävän laaja ja monipuolinen sekä riittävän usein toteutettu koko henkilöstön koulutus. Riittävät resurssit. Erityisesti organisaation johdon kouluttaminen kyberpoikkeamien hallinnan johtamiseen.
WAF, XDR, single sign-on, varmuuskopiot, SOC / detection, järjestelmien ja verkkojen arkkitehtuurisuunnittelu, secure software development lifecycle
SOC & SOAR määrämuotoinen hallinnollinen malli
Palomuurit, SIEM ja erilaiset anomalioiden tunnistukseen liittyvät järjestelmät
Tekoälyn hyödyntäminen

Vapaa sana. Voitte laittaa tähän ajatuksianne ja palautetta kyselyn aihealueeseen ja tutkimusaiheeseen liittyen.
Vastaajien määrä: 10

Vastaukset
Olisin kaivannut alkuun termin "kyberturvallisuus" määritelmää tässä kyselyssä. Voi tarkoittaa eri vastaajille aivan eri asioita, millä voi olla vaikutuksia tämän tärkeän aiheen tutkimukseen. Mutta todellakin siis mielestäni erittäin tärkeä aihe ja kiitos, että siihen panostat!
Olisi mielenkiintoista, jos saisimme tutkimuksen paljonko oikeasti resursseja eri kokoiset organisaatiot käyttävät tieto- ja kyberturvallisuuden varmistamiseen. Samalla olisi hyvä tutkia, että miten käytetyt resurssit korreloivat poikkeamien määrään. Meillä on jonkun verran subjektiivisia kyselytutkimuksia (kuten tässäkin kyselyssä), mutta tiedossa ei ole, että Suomessa olisi tehty tutkimusta, jossa olisi kysytty absoluuttisia määriä. Australiassa ACSC on tehnyt esim vastaavan selvityksen paikallisten PK-yritysten resursseista.
Työntekijät harvoin ymmärtävät oman vapaa-ajan toimintansa mahdollista vaikutusta työnantajaan. Kyberuhat rinnastetaan myös liian suuresti vain "IT asiaksi" eikä nähdä kyber-fyysistä maailmaa
Hyvä aihe, ehkä hieman hankala itsellä vastata kun olen järjestelmäasiantuntijatasolla, en niinkään yleisesti tietoturvan kanssa tekemisissä. Mutta tunnistan ongelman esim. siltä osin, että itse en osannut 2 ja 3 osioihin oikein sanoa mitään. Yrityksessä ei nimenomaan jaeta aktiivisesti tietoa mistä dokumentaatio löytyy ja mikä on tapa toimia kun jotain tapahtuu tai luullaan tapahtuvan. Meillä myös toimittaja on hieman "laiska" näissä asioissa.

Markkinoille enemmän penetraatiotestejä suorittavia yrityksiä - voi valita eri tason toimijoista organisaation omien tarpeiden mukaan.
Kyberturvan ymmärtäminen ja hyökkäystekniikkojen ymmärtäminen auttaa.
Tärkeä ja aina niin ajankohtainen aihe. Toivottavasti ei osu tuulettimeen, kun pähkäillään tekemisiä
Suomessa erityisesti kriittiseen infrastruktuuriin liittyvät yritykset ovat suhteellisen hyvin varautuneita, mutta eri sektoreiden sisällä ja erityisesti niiden välillä on merkittävää hajaannusta. Keskiarvo ei riitä, vaan hyvin ja huonosti varautuneiden organisaatioiden tulee päästä lähemmäs toisiaan. Johtamisen merkitystä ei voi korostaa liikaa, ja johdon sitoutuminen sekä vastuut tulee olla kunnossa. Lisäksi viestinnän merkitys sekä kriisittömässä että kriisitilanteessa (rauhoittelu, oikea-aikaisuus, varmuus, ohjeet jne) tulee saada saumattomasti osaksi jatkuvuudenhallintaa, mutta se korostuu kyberpoikkeamissa, kun uhkaympäristö tällä hetkellä suuntaa ajatuksen välittömästi Venäjän toimintaa, vaikka kyseessä todennäköisesti on haktivisti tai rikolliset.
Regulaatiot ja lainsäädäntö on yhä merkittävämmissä määrin ohjaamassa toimintoja aiheen kannalta parempaan suuntaan.
Kiitos - toimi hyvin!