LAUREA

AMMATTIKORKEAKOULU

University of Applied Sciences

LAUREA-JULKAISUT | LAUREA PUBLICATIONS | 191

Harri Ruoslahti (toim.)

Jatkuvuutta turvaamassa

– Laurean YAMK opiskelijoiden näkökulmia

Kannen kuva: Klas Tauberman on Pexels
Sivun 5 kuva: Fern M. Lomibao on Unsplash
Sivun 9 kuva: Gerd Altmann on Pixabay
Sivun 11 kuva: Michael Shannon on Unsplash
Sivun 12 kuva: Harri Säynevirta Kuvia Suomesta
Sivun 20 kuva: Joona Kotilainen Kuvia Suomesta
Sivun 23 kuva: Gordon Johnsson on Pixabay
Sivun 32 kuva: Burst on Negative Space
Sivun 47 kuva: Tim Mossholder on Pexels
Sivun 49 kuva: Gerd Altmann on Pixabay
Sivun 51 kuva: Nejc Soklič on Unsplash
Sivun 53 kuva: Paul Brennan on Pixabay
Sivun 67 kuva: Pete Linforth on Pixabay
Sivun 69 kuva: Pete Linforth on Pixabay
Sivun 74 kuva: Shawn Stutzman on Pexels
Sivun 83 kuva: Guillaume Périgois on Unsplash
Sivun 85 kuva: Matt Bango on StockSnap
Sivun 89 kuva: Maarten van den Heuvel on Unsplash
Sivun 96 kuva: Gerd Altmann on Pixabay
Sivun 101 kuva: Ashkan Forouzani on Unsplash

ISSN-L 2242-5241
ISSN 2242-5225 (verkko)
ISBN: 978-951-799-651-8 (verkko)

Harri Ruoslahti (toim.)

Jatkuvuutta turvaamassa

– Laurean YAMK opiskelijoiden näkökulmia

SISÄLLYSLUETTELO

Johdanto

Harri Ruoslahti

TOIMINNAN JATKUVUUDEN VARMISTAMINEN, jatkuvuuden hallinta ja resilientti toiminta ovat keskiössä Laurean tutkinnoissa Turvallisuus ja riskienhallinta, Safety, security and risk management (AMK) ja Turvallisuusjohtaminen (YAMK).

Tämän julkaisun Jatkuvuutta turvaamassa – Laurea YAMK opiskelijoiden näkökulmia artikkelit ovat kirjoittaneet Laurea YAMK Turvallisuusjohtamisen opintojakson Toiminnan jatkuvuuden varmistaminen opiskelijat ja opettajat.

Opiskelija-artikkelit on toteutettu yhteiskehittämisenä. Opiskelijat etsivät henkilökohtaisina tehtävinä neljä jatkuvuuden hallintaa käsittelevää akateemista artikkelia tai raporttia. Näistä koottiin kaikille jakso opiskelijoille yhteiskäyttöinen lähdekirjallisuuslista. Opiskelijat myös haastattelivat kukin toiminnan jatkuvuuden asiantuntijaa. Tiimeissä opiskelijat valitsivat kullekin artikkelille näkökulman ja näin yhteiskehittelivät julkaisuun tulleet artikkelit.

Artikkelin yhteiskirjoittaminen tähän julkaisuun auttaa osaltaan saavuttamaan Turvallisuusjohtaminen opintojakson oppimistavoitteita: johtaa liiketoiminnan ja teknisen infrastruktuurin toiminnan riskienmäärittelyyn ja hallintaa liittyviä toimenpiteitä, tunnistaa organisaation kriittiset toiminnot ja arvioida niiden resurssien tärkeysluokittelua, määrittää vastuut toiminnan häiriöttömyyden varmistamiseksi ja osaa johtaa toipumissuunnittelua erilaisten tunnistettujen häiriötilanteiden varalle, sekä tuottaa liiketoiminnan ja teknisten järjestelmien toiminnan jatkuvuussuunnitelmia, hallinnoida niitä sekä järjestää käytännön testausta. Taustalla tehty lähdekirjallisuuden hakeminen, jatkuvuuden asiantuntija haastattelu sekä yhteiskirjoitettu artikkeli, yhdessä opintojakson muiden tehtävien kanssa, toteuttavat Laurean Learning by Developing -oppimisperiaatetta.

1 Toiminnan jatkuvuutta turvaamassa

Visa Katajisto, Marko Kauppinen, Ian Kúrten, Markus Kärkkäinen, Teemu Niemelä & Aleksi Peurala

JOHDANTO

TÄSSÄ ARTIKKELISSA KÄSITELLÄÄN ennakkosuunnittelun merkitystä toiminnan jatkuvuudessa osana jatkuvuudenhallintajärjestelmää, tapahtumista oppimisen kannalta sekä siirtymisenä ennakkosuunnitelmista toimenpidesuunnitelmiin. Artikkelissa lähestytään aihetta myös henkilöstön kannalta, osana jatkuvuuden hallintaa sekä harjoittelun merkitystä toiminnan jatkuvuuden varmistamisessa.

Artikkeli pohjautuu pitkälti valmistavan teollisuuden yritysten näkökulmaan jatkuvuudenhallinnasta. Lähteinä on käytetty riskienhallinnan alan kirjallisuuslähteitä sekä asiantuntijahaastatteluja. Haastateltavina oli HR-johtaja teollisuuden ja rakentamisen työvälinevalmistamisen pohjoismaisesta yrityksestä sekä LVI-toimialaan liittyvä, maahantuontiin sekä markkinointiin liittyvän yrityksen edustaja.

Viimeisten kolmen vuoden aikana on maailmassa nähty tapahtumia, jotka ovat vaikuttaneet kaikkien organisaatioiden toimintaan tavoilla, joita ei kovin moni ole osannut ennustaa ainakaan toteutuneessa mittakaavassa. Maailmanlaajuinen pandemia on esiintynyt kyllä monen riskikartoituksen sivuilla, mutta kuinka moni organisaatio todella oli kehittänyt valmiiksi toimintamallit sen varalle?

Ihmisten ja materiaalin liikkuminen joko estyi tai hankaloitui ja hidastui, työvoiman saatavuus vaikeutui ja yhteiskuntien toimintojen alasajo aiheutti akuutin taloudellisen laman. Joidenkin organisaatioiden positiivinen riski toteutui ja tuloksena oli kukoistava toiminta, ainakin kunnes kilpailijat ehtivät apajille. Pandemia ei ole vieläkään ohitse, eivätkä maailman markkinat ole sen jäljiltä pystyneet vielä palaamaan normaaliin toimintaan. Taloudellisen romahduksen torjuntatoimet ovat velkaannuttaneet toimijoita aina valtiotasolta pienimpiin yrityksiin ja organisaatioihin saakka.

Pandemian jäljiltä horjuvan kasvun uralle lähtenyt talous on nyt kärsinyt uuden shokin Venäjän hyökättyä Ukrainaan. Ennennäkemättömän kovat talouspakotteet Venäjää kohtaan sekä läntisen maailman yritys eristää Venäjä maailmantaloudesta ovat vaikuttaneet suuresti maailmanmarkkinoiden tilanteeseen. Yritykset ennakoida tulevaa kehitystä ovat hankalia, sillä kukaan ei vielä tiedä, miten esimerkiksi Kiina tulee käyttäytymään lännen ja Venäjän välisen ristivedon kohteena, tai miten energiamarkkinat kehittyvät mahdollisten lisäsanktioiden myötä. Pahimmillaan maailmanmarkkinat polarisoituvat lännen ja Venäjän, Kiinan sekä Intian muodostaman idän kauppablokin väliseksi taisteluksi. Tässä haastavassa ympäristössä organisaatioiden tulisi kuitenkin kyetä menestyksekkääseen jatkuvuuden hallintaan, jonka tavoitteena on taata organisaation kyky pitää yllä riittävää resilienssiä.

ENNAKKOSUUNNITTELU OSANA JATKUVUUDENHALLINTAJÄRJESTELMÄÄ

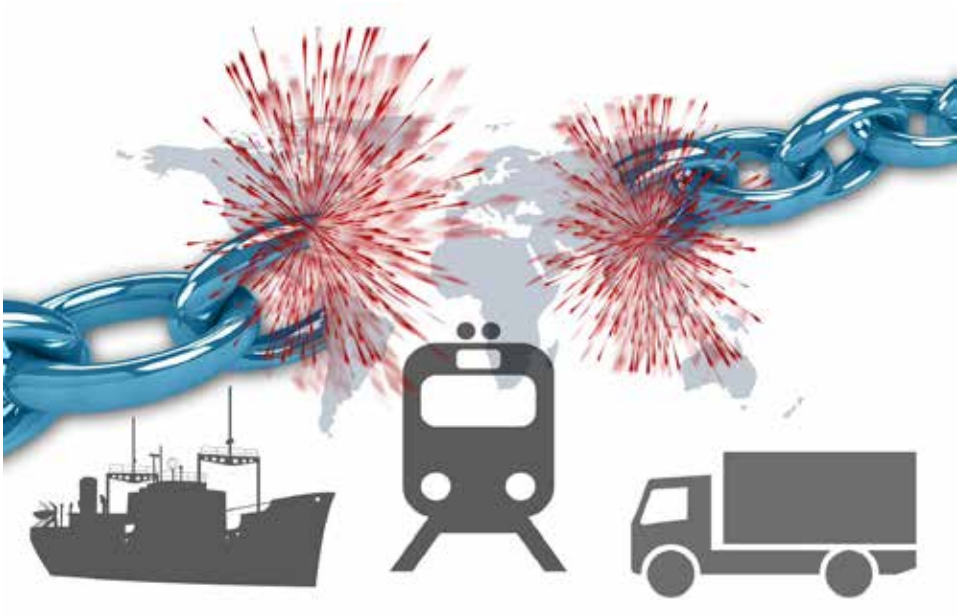
Organisaatioiden resilienssin kehittämisen ytimessä on jatkuvuuden hallintajärjestelmä, joka toimii PDCA-syklillä (plan, do, check, act) eli suunnittele, toteuta, arvioi ja toimi. Syklin ensimmäinen osa eli ennakkosuunnittelu on tässä jatkuvassa kiertokulussa tärkein vaihe. Prosessi, jossa tunnistetaan ja analysoidaan kriittiset toiminnot ja riskit, joita toiminnan jatkuvuuteen liittyy, on suoritettava vähintään vuosittain. Jatkuvuuden hallintaan on sitoutettava koko organisaatio ja henkilökunta on sitoutettava sen toteuttamiseen. (HR-johtaja 2022.)

Suunnitteluvaiheessa yrityksen tai organisaation tulee tunnistaa tärkeimmät sidosryhmänsä, niiden tarpeet ja odotukset, lakien ja viranomaisvaatimusten velvoitteet sekä asettaa jatkuvuuden hallintajärjestelmän tavoitteet. Suunnitteluvaihe käsittää myös organisaation tarvitsemien resurssien, osaamisten, dokumentoidun tiedon ja viestinnän määrittelyt. Vastuut, valtuudet ja toimintaperiaatteet tulee yksilöidä. Johdolla on keskeinen rooli ja sen tulee sitoutua jatkuvuuden hallintajärjestelmän noudattamiseen. (ISO SFS-EN 2020.)

VAIKUTUSTEN MINIMOIMINEN

Toiminnan jatkuvuuden varmistamisessa keskeistä on negatiivisten vaikutusten minimoiminen. Tässä merkittäviä toimenpiteitä ovat aiemmin tapahtuneista poikkeamista opitut tai poikkeamiin varautumisen kannalta suunnitellut toimenpiteet. Suunnittelulla on tärkeä rooli pyrittäessä vahinkojen minimoimiseen ennakointiin. Toiminnan jatkuvuuteen negatiivisesti vaikuttavaan tapahtumaan ennakoimisessa tavoitteena on tilanne, jossa esimerkiksi korkean riskin vaikutuksia toimintaan voidaan kompensoida varautumalla tapahtumaan vastaavasti korkealla resilienssillä. Tällä pyritään riskin toteutuessa minimoimaan toiminnan vaikutuksia (Linkov, Bridges, Creutzig ym. 2014).

Käytännössä tämä voidaan toteuttaa esimerkiksi siten, että tuotteita valmistavat yritykset voivat jakaa toimintaansa useisiin tuotantolaitoksiin, joissa käytettävät valmistusmenetelmät ovat keskenään yhteensopivia. Näin saman tuotteen valmistus voidaan aloittaa toisessa tehtaassa joustavasti, mikäli toiminta on keskeytynyt tai vaikeutunut alun perin tuotetta valmistaneessa tuotantolaitoksessa. Edellä mainitulla tavalla toimittaessa voidaan toiminnan jatkuvuutta varmistaa paikallisesta tuotannon häiriöstä huolimatta (Markkinointijohtaja 2022).



Markkinointijohtaja (2022) toteaa, että mikäli yrityksellä on kattava tuotevalikoima, yksittäiset tuotehäiriöt eivät pysäytä yrityksen toimintaa totaalisesti vaan sitä voidaan jatkaa yrityksen muiden tuotteiden varassa. Tähän liittyy olennaisesti myös standardin ohjaama toiminta yrityksessä. Toteutettaessa liiketoiminnan jatkuvuuden hallintajärjestelmää käyttämällä standardissa olevia elementtejä on yrityksellä mahdollisuus vähentää oleellisesti häiriöstä johtuvia kustannuksia ja vahvistaa organisaation kriisinkestävyyttä kokonaisuutena sekä parantaa sidosryhmien luottamusta organisaation kyvykkyyteen (ISO SFS-EN 2020).

Toiminnan jatkuvuuden varmistamisen suunnittelun tuloksena voidaan toimintamalleista ja -tavoista koostaa yritykselle oma jatkuvuuden hallinnan käsikirja. Tähän voidaan kerätä toimenpidesuunnitelmien lisäksi muun muassa toimintamallit kriisitilanteita varten, pelastussuunnitelmat sekä toipumissuunnitelmat. Hyvin koostettua jatkuvuuden hallinnan käsikirjaa voidaan tarjota käyttöön myös sidosryhmille. Yhteistyöverkosto voi tällöin samoja toimintamalleja omaksumalla vahvistaa toisiaan kustannustehokkaasti. (HR-johtaja 2022.)

Agnieszkan & Werbinska-Wojciechowskan (2021) mukaan yritykset voivat kehittää sisäisiä riskienhallintaprosesseja yhdistämällä toimitusketjun riskienhallinnan sekä organisaation kypsyysmallinnuksen. Yritykset hyötyvät myös tästä toimitusketjun tiedon yhdistämisestä. Riskien hallinnan kypsyyttä ja logistisia prosesseja tutkivassa artikkelissaan Agnieszka esittelee yritysten riskihalukkuutta logistisissa prosesseissa yhdistettynä toimitusketjun osallistumiseen jaetun riskin kannalta. Tutkimus osoitti, että viisi määriteltyä "kypsyys"aluetta (tieto, riskiarvio, prosessien riskihallinta, riskin jakaminen sekä riskiseuranta), mahdollistavat moniulotteisen diagnoosityökalun riskihalukkuuden tunnistamiseen.

Markkinointijohtaja (2022) korostaakin, että toimitusketjun osalta toimijaverkosto on usein luotu korvaamaan mahdollisia häiriöitä. Raaka-aineiden osalta yrityksellä saattaa olla useita toimittajia, mutta esimerkiksi kalusteiden osalta valmistajaverkoston rakentaminen on alihankkijoiden varassa. Tällöin myös raaka-aineiden saatavuus jälkimmäisten osalta korostuu.

ISO 22313 standardissa mainitaan toiminnan jatkuvuudesta mm. seuraavasti: *"liiketoiminnan jatkuvuuden hallintajärjestelmä parantaa organisaation valmiutta jatkaa toimintaa häiriöiden aikana".* Toimittaessa tällä edellä mainitulla tavalla, yrityksellä on mahdollisuus lisätä ymmärrystä yrityksen sisäisistä ja ulkoisista suhteista sekä kehittää viestintää myös sidosryhmien osalta. Näiden lisäksi voidaan luoda edellytyksiä ympäristölle, jossa myös toiminnan jatkuva parantaminen on mahdollista. (ISO SFS-EN 2020.)

Tarkasteltaessa esimerkiksi yksittäisen yrityksen toimintaa konsernitasolla, raaka-aineiden saatavuuden varmistaminen toteutetaan hankkimalla raaka-aineita usealta eri toimittajalta sekä erilaisin varastojärjestelyin. Raaka-ainetoimittajien osalta järjestely rakentuu ns. päätoimittajan ja muiden raaka-ainetoimittajien kanssa toteutettuun järjestelyyn, jossa eri toimittajilta hankitaan erilaisia osuuksia suunnitelman mukaisesti. Tällä taataan raaka-aineen jatkuva saatavuus eikä toimitusketju rakennu vain yhden raaka-ainetoimittajan varaan. (Markkinointijohtaja 2022.)

Toimittajien valinta on yksi merkittävistä toiminnan jatkuvuuteen liittyvistä tekijöistä. Vahva toimittajabrändi ja yleisesti tunnettu toimittaja lisää toimittajaluotettavuutta. Joka tapauksessa toimittajat on auditoitava sekä heidän toimintansa kriisitilanteissa on varmistettava vahvasta brändistä huolimatta. Lisäksi mukautumiskykyyn vaikuttavat jatkuva tuotekehitys sekä markkinoiden tuntemus. (Markkinointijohtaja 2022.)

Jatkuvuuden varmistaminen työtekijöiden osalta voidaan toteuttaa nimettyjen seuraajien ja varahenkilöiden kartoittamisella. Tällä toimenpiteellä varmistetaan osaamisen säilyminen ja siten myös toiminnan jatkuvuus. Näissä toiminnan jatkuvuutta turvaavissa toimenpiteissä korostuvat myös toistuvat analyysit sekä oman toiminnan edelleen kehittäminen. Lisäksi tärkeää on myös ennakointi, esimerkiksi ympäristövaatimusten osalta sekä säädösten tunteminen ja yleinen toiminnan harmonisointi. Esimerkiksi jonkin raaka-aineen kieltäminen jossakin EU-maassa tarkoittaa, että se tulee kielletyksi todennäköisesti myös muualla. (Markkinointijohtaja 2022.)

Pandemia on vaikuttanut komponenttien saatavuuteen, jolloin jopa puolet valmistavista yrityksistä joutuu luopumaan JIT (just in time) -periaatteesta, jossa materiaaleja ei varastoida. Yritysten on harkittava puskurivaraston luomista, sillä toimituksissa on voimakasta vaihtelua. Maailmanlaajuiset kuljetukset ovat myös kriisissä sekä konttipulan että kohonneiden kuljetuskustannusten vuoksi. Neljä viidestä valmistavista yrityksistä aikoo vähentää riippuvuuttaan pitkistä logistiikkaketjuista. (Slowik 2022.)

Varastoinnin tärkeys korostuu monella eri toimialalla. Haastattelussa olevassa yrityksessä on käytössä eurooppalaisen konsernin toimintamalli, jossa toimitukset kohdistuvat pääasiassa suoraan jälleenmyyjille. Tässä mallissa mahdollisten viivästysten ja toimitusvaikeuksien osalta korostuu kuitenkin myös tarve logistiikkakeskukselle. Suomessa tällainen paikallisvarasto toimii ns. puskurivarastona, jolloin toimitukset eteenpäin eivät viivästy, vaikka tuotetta ei olisikaan saatavissa kyseisellä hetkellä tuotantolaitokselta. Varastoa myös kasvatetaan tarvittaessa, jotta valmius tuotteiden toimittamiseen edelleen jälleenmyyjille säilyy. (Markkinointijohtaja 2022.)

TAPAHTUMISTA OPPIMINEN

Riskienhallintaan kiinteästi liittyvä PDCA-toimintamalli ei ole ainut syklinen arviointimalli toiminnan tuloksellisuuden arvioinnille. Toinen läheinen, mutta hieman eri painotuksella oleva toimintamalli on PIML, (Plan, Implement, Measure, Learn). PIML malli korostaa PDCA:ta hieman voimakkaammin vielä arvioimisen ja oppimisen merkitystä riskienhallintaprosessissa. (Hopkin 2018, 108.) PIML metodi on valittu mukaan the Committee of Sponsoring Organizations (COSO) yritysriskienhallinnan malliin (COSO Enterprise Risk Management cube) ja riskienhallinnan kehykseen (COSO Enterprise Risk Management framework 2017) kuvaamaan toiminnan arvioinnin prosessia (IRM). Huolimatta siitä, mitä lyhennettä tai keskenään hyvin samankaltaista metodia käytetään, on pääasia, että toimintaa toteutetaan ja arvioidaan systemaattisesti. PDCA tai PIML lyhenteiden takaa löytyvät menetelmät ja metodit ovat kuitenkin riskienhallinnan maailmassa laajalti tunnistettuja tunnustettuja. (Hopkin 2018, 437.)

Kun PIML mallista ensiksi erotetaan M, eli measuring (mittaaminen), tarkoitetaan sillä tässä yhteydessä riskienhallinnan toimenpiteiden tehokkuuden mittaamista ja riskitietoisen kulttuurin sekä riskienhallinnan organisaatiossa sijoittumisen arviointia. Työkaluna tähän tehtävään voidaan käyttää riskienhallinnan puolelta esimerkiksi vaikutusanalyysiä (Business Impact Analysis, BIA) sekä riskiviestintää (risk communication). L kuvastaa toimintona sanaa learning (oppiminen) ja tällä tarkoitetaan tarkkailua sekä riskienhallintatoimenpiteiden onnistumisen arviointia. Auditointi on tässä toiminnassa hyvä työkalu, myös erilaisten riskiraporttien tarkastelu kuuluu osaksi oppimisvaihetta. (Hopkin 2018, 439.)

Hopkinin (2018, 289) mukaan organisaation hyvään riskienhallintakulttuuriin kuuluu olennaisesti myös oppimisen kulttuuri. Tapahtumista oppiminen ja organisaation johdon sitoutuminen toimintaan on keskeinen osa menestyksekästä riskienhallintaa. Haittatapahtumista tai läheltä piti -tilanteista raportoiminen ja niistä oppiminen ei kuitenkaan ole ainut tapa lähestyä oppimista riskitietoisissa ja korkeankaan turvallisuustason organisaatioissa. Lähes päinvastainen lähestymistapa on erinomaisuudesta oppiminen, eli Learning from Exellence (LfE).

LfE on viime aikoina varsinkin lääke- ja hoitotieteen puolella esiin noussut ja toteutettu menetelmä, jossa keskitytään poikkeamien ja riskien sijaan hyvin toteutuneisiin tapahtumiin ja niiden raportointiin. Tavoite on, että henkilöstö itse tai vertaiset toiminnanharjoittajat läheisistä sidosryhmistä raportoivat organisaation määrittämälle taholle toisten työntekijöiden tai organisaation toimiyksiköiden onnistumisista. Nämä onnistumiset ja hyvät suoritukset analysoidaan ja kokemukset jaetaan organisaation käyttöön ja hyödyksi. (Kelly, Blake & Plunkett 2016.)

Erilaiset yleisesti käytössä olevat standardit määrittelevät ja asettavat myös tavoitteita organisaation oppimiselle. Laadunhallintaa käsittelevä standardi SFS-EN ISO 9001 sisältää omat osionsa jatkuvasta parantamisesta organisaation tietämyksen ylläpidosta. Osana laadullisesti hyviä tuotettavia palveluita ja tuotteita pidetään jo aiemminkin mainittua tapahtumista oppimista ja niiden raportoinnin kautta saadun tiedon hyödyntämistä. Riskienhallinnan standardi SFS-EN ISO 31000 listaa myös nämä samat osa-alueet kiinteiksi ja välttämättömiksi osiksi kokonaisuutta.

ENNAKKOSUUNNITTELUSTA TOIMENPIDESUUNNITELMIIN

Ennakkosuunnittelun on hyvä olla osana päivittäistä tekemistä. Pelkästään analysoimalla mahdollisia tulevaisuuden häiriötilanteita sekä varautumista ei johda itse häiriötilanteiden hallintaan. Tarvitaan myös käytännön toimenpiteitä sekä harjoittelua ennakkosuunnitelmien toimenpiteiden toteamiseen sekä toimimiseen erilaisissa häiriötilanteissa. Jatkuva tilanteen tasalla oleminen sekä kaikkien mahdollisten skenaarioiden (myös epätodennäköisten) käsittely sekä tarvittavat valmistelevat toimenpiteet ovat ensisijaisen tärkeitä ennakkosuunnittelussa tämän lisäksi tarvitaan toimintaohjeita sekä menetelmiä häiriötilanteissa toimimiseen. Toiminnan pitää olla keskeytyksetöntä ja jatkuvaa. Liiketoiminta ei saisi keskeytyä missään tilanteessa ja toiminnan on mukauduttava mahdollisiin ympäristössä tapahtuviin merkittäviin muutoksiin, jotka voivat haitata kyseisen toiminnan jatkuvuutta.

Ennakkosuunnittelussa voidaan käyttää työkaluna esimerkiksi tarkastuslistoja siitä, mitä on hyvä huomioida ja miten toimia häiriötilanteissa. Ennakkosuunnittelun ja häiriötilanteiden toimintamallien lisääntyessä on tarkoituksenmukaista tehdä järjestelmällistä raportointia eri toimintojen tilasta. Tämä edesauttaa saamaan hyvää kokonaiskuvaa siitä mitä asioita on ennakoitu ja mihin olisi hyvä vielä kiinnittää huomiota sekä miten toimitaan eri häiriötilanteessa.

Ennakkosuunnittelun myötä tuotettujen toimenpidesuunnitelmien on oltava riittävän yksityiskohtaisia, jotta pystytään toiminaan suunnitellulla tavalla häiriötilanteissa. Liian laveat toimenpiteet ja toimenpideohjeet johtavat asian käsittelyyn, mutta eivät välttämättä korjaa tai ehkäise vallitsevaa tilannetta tarkoituksenmukaisesti.

Riittävän ennakoinnin ja varautumisen tason toteamiseen tarvitaan käytännön harjoittelua. On todennäköistä, että ennakoidut toimenpiteet eivät toimi, jos kyseisiä häiriötilanteessa kohdattuja toimintatapoja ja menetelmiä ei ole harjoiteltu ja mietitty etukäteen. Kun tarvittavat ennakoidut toimintatavat ja toiminnot ovat myös koko ajan käytössä ja joita harjoitellaan säännöllisesti edesauttavat sujuvaa toimimista häiriötilanteissa. (Toimitusjohtaja 2022.)

Ennakoinnista ja vallitsevasta tilanteesta tuotettu toimiva tilannekuva auttaa näkemään paremmin kokonaisuuksia sekä kiinnittämään huomiota oleellisiin seikkoihin. Toimintamallit eivät saisi muuttua merkittävästi häiriötilanteissa. Samaa toimintatapaa on hyvä käyttää kaikissa toimintaolosuhteissa. Toimintatapojen muuttuminen merkittävästi häiriötilanteissa johtaa helposti sekavaan ja ei niin toimivaan sekä tehokkaaseen toimintaan. On hyvä pyrkiä soveltamaan aktiivisessa käytössä olevia menetelmiä ja työkaluja mahdollisimman paljon myös häiriötilanteissa kitkattoman jatkuvuudenhallinnan aikaansaamiseksi. (Toimitusjohtaja 2022.)

HENKILÖSTÖN OSAAMINEN OSANA JATKUVUUDEN HALLINTAA

Kun puhutaan yrityksen varautumisesta ja jatkuvuudenhallinnasta, ei voida sivuuttaa sitä tosiseikkaa, että yrityksen suurin yksittäinen voimavara jatkuvuudenhallinnan onnistumisessa on yrityksen henkilöstö. Huoltovarmuuskeskuksen (2022) SOPIVA-hankkeessa on kehitetty yrityksille työkaluja, joilla kehitetään toimintavarmuutta kaikenlaisten tilanteiden varalle. SOPIVA-hankkeessa on listattu viisi suositusta koskien henkilöstöä ja henkilöresurssien hallintaa:

1. Jatkuvuuden hallinnan **osaamiselle** on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään.
2. Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia.
3. Organisaatiossa on sovittu tapa toimia valvonnassa, turvallisuuspoikkeamissa ja väärinkäytöstilanteissa.
4. Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt on suunniteltu.
5. Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu vähintään ydintoimintojen jatkuvuuden hallinnan edellyttämällä tavalla.

Liiketoimintaa uhkaavat tilanteet eivät usein saavu kello kaulassa ja niihin reagoimiseen vaaditaan jatkuvaa valmiutta, joka syntyy jo valmiiden suunnitelmien säännöllisellä päivittämisellä sekä harjoittelemisella. Johdon katselmoinnit ja riippumattoman osapuolen auditoinnit ovat tärkeitä arkisia rutiineja jatkuvuudenhallinnan kannalta sekä erityisen tärkeitä silloin, kun jokin liiketoimintaprosessi muuttuu. Testaus ja harjoittelu puolestaan kehittävät varmuutta sekä kykyä toimia oikein myös ennakoimattomissa tilanteissa. Jatkuvuudenhallinta onkin hyvä sitoa osaksi organisaatioiden jokapäiväistä tekemistä, sillä se ei ole vain kertaluontoinen projekti, vaan jatkuva ja kehittyvä prosessi. (Teknologiateollisuus 2022.)

> ***Liiketoimintaa uhkaavat tilanteet eivät usein saavu kello kaulassa ja niihin reagoimiseen vaaditaan jatkuvaa valmiutta, joka syntyy jo valmiiden suunnitelmien säännöllisellä päivittämisellä sekä harjoittelemisella.***

Ilmonen, Kallio, Koskinen & Rajamäki (2016, 175) muistuttavat, että jatkuvuussuunnitelmien skenaariot harvoin toteutuvat ainakaan niin laajamittaisina kuin ne on luotu. Tämä saattaa johtaa siihen, että suunnitelmien tekeminen vaikuttaa teoreettiselta puuhastelulta ja harjoittelu turhalta. Vaarana on tällöin, että jatkuvuussuunnitelmien laatiminen jää kertaluontoiseksi työksi, eikä niitä päivitetä säännöllisesti. Johto on avainasemassa huolehtimassa, että päivityksiä tehdään ja suunnitelmia harjoitellaan riittävästi.

Myös Sterling, Duddridge, Elliott, Conway & Payne (2012, luku 10) korostavat jatkuvuussuunnitelmien ja kriisivalmiuksien kehittämiseen ryhtymisen jälkeen henkilöstön koulutuksen merkitystä. Mikäli henkilöstöä ei kouluteta siihen, mitä heiltä odotetaan, ei voida olettaa, että he toimisivat toivotulla tavalla kriisitilanteissa. Koulutus lisää henkilöstön tietoisuutta, hioo tarvittavia taitoja ja ennen kaikkea antaa henkilöstölle luottamusta siihen, että he pystyvät hoitamaan roolinsa missä tahansa tilanteessa.

Osaamisen kannalta on myös olennaista se, että usein varsinkin pienemmissä organisaatioissa osaaminen henkilöityy ja avainhenkilöiden irtisanoutuessa organisaatioon saattaa muodostua koko liiketoimintaa vaarantavaa osaamisvajetta. Siksi jatkuvuudenhallinnan kannalta olisi suotavaa, että eri rooli- ja tehtäväkohtaiset vastuut olisi dokumentoitu ja osaaminen kahdennettu siten, että jokaisessa avainroolissa olisi nimettynä varahenkilö. (Suomen riskienhallintayhdistys 2022.)

Lindstedt & Amour (2017, luku 1) puolestaan korostavat sitä ristiriitaa, joka syntyy organisaatioiden luodessa jatkuvuussuunnitelmiaan dokumentteihin pohjautuvina ohjeistuksina. Ne saattavat luoda eräänlaisen tunnelinäön katsoa jatkuvuudenhallintaa vain näiden dokumenttien valossa ja luoda käsityksen siitä, että tietojen dokumentointi on valmiuden ydin. Tämä siirtää huomion painopisteen teoriassa tehtäviin toimenpiteisiin ja jättää huomioimatta kriisiosaamista, joka on jatkuvuudenhallinnan kannalta merkittävää.

Lindstedt & Amour (2017, luku 1) kritisoivat myös sitä, kuinka liika keskittyminen dokumenttien laatimiseen jättää suurelta osin huomioimatta työntekijöiden psykologisien kykyjen parantamisen kriiseissä toimimiseksi. Nämä valmiiksi luodut dokumentit vähentävät lisäksi joustavuutta ja innovatiivisuutta kriisien aikana, koska ihmiset pyrkivät tekemään sen, mikä on heille kirjoitettu sen sijaan, että he ryhtyisivät luoviin ongelmanratkaisuihin käsitelläkseen muuttuvaa kriisin jälkeistä ympäristöä.

On liian pitkälle vedetty ajatus luopua dokumentteihin pohjautuvista jatkuvuussuunnitelmista, mutta on kuitenkin hyvä muistaa ihmisten vaihteleva käyttäytyminen paine- ja kriisitilanteiden alla. Jatkuvuussuunnitelmat menettävät huomattavasti potentiaaliaan, mikäli henkilöstö ei ole harjoitellut niitä toimintoja, joita heiltä odotetaan kriisitilanteissa. Paperilla ne toiminnot, jotka ovat johtajille selkeitä lukuisten jatkuvuudenhallintaan liittyvien suunnittelupalaverien jälkeen, eivät ole yhtä selkeitä suorittavalle portaalle. Kriisitilanteissa usein tarvittavat toimet eivät kuitenkaan eroa juurikaan arkisista tehtävistä, mutta ne tehdään poikkeuksellisissa olosuhteissa. Ja näissä olosuhteissa toimimista on harjoiteltava samojen ihmisten kanssa, joiden kanssa tehdään normaalioloissakin töitä. Autenttisista harjoituksista on myös mahdollista kerätä käytännöntietoa, kuinka valmiussuunnitelmat käytännössä toimivat. (Johnson 1977, luku 4.)

Organisaation kykyä toimia jatkuvuutta uhkaavissa tilanteissa korostaa myös se, että organisaatiossa on yhtenäinen yrityskulttuuri ja johto tiedostaa, että yrityskulttuuria on rakennettava systemaattisesti. Yrityskulttuuri ohjaa kaikkea toimintaa ja siksi on tärkeää, että se kannustaa työntekijää noudattamaan ja kehittämään hyvää turvallisuuskulttuuria. Sanotaan, että yrityskulttuuri on se mitä tapahtuu silloin kun kukaan ei ole katsomassa. Henkilöstön motivaatio ja asenne ratkaisee. (Leidenschaft 2022.)

Erään määritelmän mukaan motivaatio on psyykkinen tila, jonka mukaan määräytyy tekemisen kohde ja vireys. Se muodostuu henkilön haluista ja tarpeista eikä sitä voida antaa ulkopuolelta. Organisaatio voi toki pyrkiä luomaan motivoivan ympäristön herättämään työntekijöiden motivaation. Tässä yrityksen johdolla on avainasema. Siksi tärkein seikka, johon johtajan tulisi nykypäivänä kiinnittää huomiota, on se kuinka lahjakkaat, yrityksen ns. vanhat työntekijät pysyvät yrityksessä. Kun puhutaan henkilöstöstä ja sen hyvinvoinnista, ei voida sivuuttaa hyvää johtamista, sillä lopulta kaikki ongelmat ovat johtamisongelmia. Siksi jatkuvuudenhallinta on mitä suurimmassa määrin myös HR-asia.

JOHTOPÄÄTÖKSET

Riskienhallintaan liittyvän ennakkosuunnittelun toteutus ja mieltäminen osaksi mitä tahansa liiketoiminnan tai muun toiminnan harjoittamista on ensiarvoisen tärkeää toimivaa ja toimintavarmaa toiminnanjatkuvuuden kokonaisuutta tavoiteltaessa. Erilaiset riskikartoitukset ja riskienhallintatoimet auttavat ymmärtämään ja ehkäisemään negatiivisia lopputulemia. Toimenpiteiden harjoittelu ja selkeät toimintamallit poikkeamatilanteisiin puolestaan auttavat toipumisessa ja toiminnan jatkamisessa haitallisen tapahtuman jälkeen. Toiminnan tarkastelu henkilöstön inhimillisen toiminnan näkökulmasta sekä jo mahdollisesti aiemmin tapahtuneiden haittatapahtumien näkökulmasta, ja niistä oppimalla, voidaan myös vahvistaa, kehittää ja parantaa organisaation toimintaa.

Osaava henkilöstö minkä tahansa organisaation tukijalkana tulee sitouttaa ja perehdyttää toimimaan myös riskienhallinnan näkökulmat huomioon ottaen. Kyvykäs ja motivoitunut henkilöstö torjuu ennalta erilaiset haitalliset tilanteet ja poikkeamat, mutta myös kykenee reagoimaan niihin niiden realisoituessa. Reagoinnissa tärkeää on aikaansaavien ihmisten lisäksi toimiva organisaatiorakenne, jossa kyvykkäät ihmiset kykenevät suorittamaan vaadittavia toimenpiteitä myös poikkeavissa tilanteissa. Ennakkovalmistautuminen, suunnittelu, sekä toimenpiteiden harjoittaminen lisäävät tätä kyvykkyyttä.

Lähteet

Agnieszka A. T. & Werbinska-Wojciechowska, S. 2021. Risk Management Maturity Model for Logistic Processes. Sustainability 13 (2), 659.

Hopkin, P. 2018. Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. London: Kogan Page Ltd.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2016. Johda riskejä: käytännön opas yrityksen riskienhallintaan. Toinen laitos. Helsinki: Finva.

Institute of Risk Management 2018. From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks. London: Institute of Risk Management.

ISO SFS-EN 2015. ISO 9001:2015 Laadunhallintajärjestelmät.

ISO SFS-EN 2018. ISO 31000:2018 Riskienhallinta.

ISO SFS-EN 2020. ISO 22313:2020 Turvallisuus ja kriisinkestävyys.

Johnson, T. 1977. Crisis leadership : how to lead in times of crisis, threat and uncertainty. London, U.K: Bloomsbury Business.

Kelly, N., Blake, S. & Plunkett A. 2016. Learning from excellence in healthcare: a new approach to incident reporting. Arch. Dis. Child, 101 (9),788-91.

Leidenschaft 2022. Yrityskulttuuri. Viitattu 12.4.2022. *https://leidenschaft.fi/yrityskulttuuri/*

Lindstedt, D. 2017. Adaptive Business Continuity: A New Approach. Brookfield, Connecticut USA: Rothstein Publishing.

Linkov, I., Bridges, T., Creutzig, F. et al. 2014. Changing the resilience paradigm. Nature Clim. Change 4, 407–409. *https://doi.org/10.1038/nclimate2227*

Suomen riskienhallintayhdistys 2022. PK-RH-riskienhallinta. Avainhenkilöriskit. Viitattu 12.4.2022 *https://pk-rh.fi/riskien-luokittelu/operatiiviset-riskit/henkiloriskit/avainhenkilot.html*

Slowik, M. 2022. Six ways manufacturing will prove its resiliency in 2022. Manufacturing.net. *https://www.manufacturing.net/economics/blog/22044049/six-ways-manufacturing-will-prove-its-resiliency-in-2022*

Sterling, S. 2012. Business Continuity For Dummies. Hoboken New Jersey: John Wiley & sons.

Teknologiateollisuus 2022. Varaudu ennalta häiriötilanteisiin. Viitattu 11.4.2022. *https://teknologiateollisuus.fi/fi/tyomarkkinat/yritysturvallisuus/varaudu-ennalta-hairiotilanteisiin*

Toiminnan on aina jatkuttava 2022. Helsinki: Huoltovarmuuskeskus. *https://www.huoltovarmuuskeskus.fi/files/d12f974dd7816360746a5a6343b7ceadeb60ceab/sopiva_esite.pdf*

Julkaisemattomat lähteet

HR-johtaja 2022. Asiantuntijahaastattelu 10.2.2022.

Markkinointijohtaja 2022. Asiantuntijahaastattelu 7.3.2022.

Toimitusjohtaja 2022. Asiantuntijahaastattelu 4.3.2022.

2 Asiantuntijoiden kokemuksia toiminnan jatkuvuuden varmistamisesta

Sanna Koenkytö, Noora Koivu, Tehi Palletvuori, Anna-Riitta Piirainen & Laura Ranne

TÄSSÄ ARTIKKELISSA KÄYMME läpi erilaisia liiketoiminnan keskeytystilanteita ja näiden tilanteiden ehkäisemistä sekä resilienssin varmistamista. Lisäksi pohdimme jatkuvuuden varmistamisen ulottamista toimijaverkostoon. Lopuksi tarkastelemme jatkuvuuden varmistamista uhkaavia tekijöitä sekä esille tulleita toimenpidesuosituksia. Aineistona artikkelissa on käytetty viiden jatkuvuudenhallinnan asiantuntijan haastatteluja ja aiheeseen liittyvää kirjallisuutta.

JOHDANTO

Pohdimme artikkelissa vastauksia kysymyksiin, miten liiketoiminnan keskeytystilanteita voidaan ehkäistä jatkuvuudenhallinnalla ja resilienssiä varmistaa. Jatkuvuudenhallinnalla tarkoitetaan niitä toimenpiteitä, joiden avulla organisaatio pystyy ennakkoon suunnitelluilla sekä toteutetuilla järjestelyillä ja johtamismalleilla hallitsemaan erilaisia toimintaansa uhkaavia häiriötilanteita. Nämä eri toimintojen jatkuvuudenhallinnan menettelyt varmistavat sen, että erilaisten rakenteellisten ja teknologisten ratkaisujen ohella organisaatio pystyy toteuttamaan tehtäväänsä ja täyttämään velvoitteensa häiriötilanteissa ja poikkeusoloissa. (Klemm & Pajala 2019, 17.) Resilienssi tarkoittaa kriisinkestävyyttä ja mukautumiskykyä niin yksilön kuin organisaation sekä yhteiskunnan tasolla (Sitra 2022; Työterveyslaitos 2022).

Viranomaisten ja elinkeinoelämän kanssa tiivistä yhteistyötä tekevä Huoltovarmuuskeskus määrittelee jatkuvuudenhallinnan tarkoittavan huoltovarmuutta parantavaa prosessia, jonka avulla yritys, järjestö, julkinen toimija tai muu organisaatio tunnistaa liiketoimintaan liittyvät uhkat, riskit, häiriötilanteet ja riippu-

vuudet. Organisaatio myös arvioi näiden uhkien vaikutuksia organisaatiossa ja sen toimijaverkostossa sekä organisoi ja toteuttaa menettelytavat mahdollisten häiriötilanteiden varalle. Osa jatkuvuudenhallintaa on myös kumppaneiden toimintakyvyn varmistaminen kriittisissä häiriötilanteissa sekä liiketoiminnan intressien suojaaminen ja kyky tuottaa arvoa. (Huoltovarmuuskeskus 2022.)

Brittiläinen standardi BS 31100:2011 määrittelee liiketoiminnan jatkuvuuden kokonaisvaltaiseksi hallintaprosessiksi, jossa tunnistetaan organisaatioon mahdollisesti kohdistuvat uhkat ja vaikutukset liiketoimintaan, joita nämä uhkat voivat toteutuessaan aiheuttaa. Liiketoiminnan jatkuvuuden hallinta tarjoaa puitteet organisaation häiriönsietokyvyn kehittämiseksi sekä valmiudet tehokkaisiin vastatoimiin keskeisten sidosryhmien, maineen, brändin ja arvoa luovan toiminnan etujen turvaamiseksi.

Tämä määritelmä on hyvin saman sisältöinen kuin yllä kuvattu Huoltovarmuuskeskuksen määritelmä. Brittiläisen standardin ja Suomessa toimivan valtion viraston yhtenevä jatkuvuudenhallinnan määritelmä on luonteva ottaen huomioon, että liiketoiminnan jatkuvuuden hallinnalla on juuret yrityssektorilla ja sillä pyritään varmistamaan organisaation kriittisten toimintojen jatkuvuus hyväksyttävällä tasolla myös häiriötilanteissa. (Hopkin 2018, 203; Cedergren & Hassel 2022, 3.)

Kaikki organisaatiot eivät voi noudattaa samanlaista jatkuvuussuunnitelmaa, koska jokaisella organisaatiolla on omat hyvät käytäntönsä. Suunnitelma toiminnan jatkuvuudesta pitää olla yksilöllisesti mietitty, jotta se palvelee tietyn organisaation tarpeita. Suunnitelman perusteet, kuten tarvekartoitus ja roolien ja vastuiden selkeyttäminen sekä organisaation johdon tuki, ovat elementtejä, jotka jokaisessa suunnitelmassa olisi hyvä olla. (Iivari & Laaksonen 2009, 92-93.)

Organisaation liiketoimintamalli ja toimintaympäristö vaikuttavat siihen, kuinka suuri työmäärä suunnitelman tekemisessä on. Työmäärään vaikuttaa se, onko tavoitteena tehdä suunnitelma, jonka tarkoituksena on kattaa kaikki yrityksen toiminnat vai esimerkiksi luoda suunnitelma tietylle prosessille organisaatiossa. Se kuinka paljon organisaatiolla on kokemusta entuudestaan toiminnan jatkuvuuden suunnittelusta, ja kuinka perehtynyt se on prosesseihin ja kuinka tarkasti tiedot on dokumentoitu vaikuttaa myös lopullisen työn määrään ja suunnitelman aikaansaamisen kestoon. (Iivari & Laaksonen 2009, 92-93.)

Tämän artikkelin pohjana on käytetty viiden eri jatkuvuudenhallinnan asiantuntijan haastattelua ja verrattu saatuja vastauksia kirjallisuuslähteisiin. Haastattelut toteutettiin puolistrukturoituina yksilöhaastatteluina. Kukin artikkelin kirjoittaja haastatteli yhtä asiantuntijaa. Haastattelujen avulla kartoitettiin asiantuntijoiden kokemuksia ja näkemyksiä toiminnan jatkuvuuden varmistamisesta, ehkäisemisestä ja keskeytysten vaikutusten minimoimisesta. Haastattelut tehtiin joko kasvokkain tai etäyhteyden kautta ja ne dokumentoitiin kirjoittamalla ylös haastateltavien vastauksia sekä haastattelijan ajatuksia haastattelujen aikana. Vastaukset koottiin lopulta analyysitaulukkoon, jossa kunkin kysymyksen vastauksista koottiin synteesi.

Kanasen (2014, 71) mukaan tutkijan on aina tulkittava haastattelussa sanottua, eikä haastattelun kautta saatava tieto näin ollen ole sellaisenaan tutkimuksen tulosta. Tutkijalta vaaditaan myös kykyä tulkita informantin kertomaa haastattelusisältöä. Haastateltavat kertoivat vaihtelevassa laajuudessa omasta taustastaan kokemuksen näkökulmasta eikä tässä artikkelissa käydä haastateltavien anonymiteetin varmistamiseksi tässä artikkelissa haastateltavien taustoja tarkemmin läpi. Yleisesti voidaan kertoa, että haastateltavat työskentelevät useilla huoltovarmuuskriittisillä aloilla julkisella ja yksityisellä sektorilla.

Haastattelukysymyksiä oli kymmenen ja ne jakautuivat haastateltavan taustan ja jatkuvuudenhallinnan kokemuksen tarkasteluun. Vastausten analysoinnissa pääteemoiksi nousivat kyberhyökkäykset, pandemia sekä työntekijöiden inhimilliset virheet. Haastattelun alkuosiossa käytiin läpi myös haastateltavien mahdollisesti kokemia liiketoimintaa keskeyttäneitä tilanteita. Toisessa osiossa haastateltavat kertoivat näkemyksiään jatkuvuuden keskeytysten ehkäisemiseksi sekä toiminnan resilienssin varmistamiselle. Toinen osio sisälsi

myös kysymyksen siitä, minkälaiset seikat haastateltava on kokenut tärkeiksi keskeytysten vaikutusten minimoimiseksi. Tässä osiossa käytiin lisäksi läpi toiminnan jatkuvuutta kyberhäiriötilanteissa. Haastattelun kolmas osio käsitteli toimijaverkoston jatkuvuuden varmistamista ja luottamuksen rakentamista toimijaverkostossa. Viimeisessä haastatteluosiossa haastateltavat kertoivat jatkuvuuden varmistamista uhkaavista riskeistä sekä toimenpidesuosituksista. Lopuksi haastateltavilta kysyttiin, mitä muuta he haluaisivat kertoa jatkuvuudenhallintaan liittyen.

LIIKETOIMINNAN KESKEYTYMISTILANTEET

Toimintaan kohdistuvat uhkat voivat olla yhteisiä kaikille, kuten globaali talouskriisi tai pandemia, tai kohdistua rajatummin esimerkiksi eri toimialoille (Iivari & Laaksonen 2009, 92-93). Uhkat voivat olla organisaation ulkopuolelta tulevia kuten ammattirikollisten tekemät kyberhyökkäykset tai ne voivat aiheutua organisaation sisällä yksittäisen työntekijän inhimillisestä virheestä (Valtiovarainministeriö 2003, 6).

Haastateltavilta kysyttiin, millaisia liiketoiminnan keskeytymistilanteita he ovat kokeneet. Yhteenvetona jatkuvuudenhallinnan asiantuntijoiden vastauksista voidaan todeta, että suurin osa toiminnan jatkuvuuden häiriöistä on liittynyt erilaisiin tietojärjestelmien tai tietoliikenteen häiriöihin ja muihin IT-ongelmiin. Vastauksissa korostui, että tietotekniset ongelmat on koettu todennäköisimmäksi uhkaksi ja ne voivat olla vaikutukseltaan hyvinkin laajoja. Lisäksi tietoteknisten häiriöiden syiden selvittäminen ja mahdollinen kadonneiden tietojen palauttaminen voi viedä paljon aikaa.

Toinen haastateltavien vastauksissa toistuva syy toiminnan jatkuvuuden häiriöihin oli yksittäisten työntekijöiden tahattomasti tekemät inhimilliset virheet. Kolmas jatkuvuuden asiantuntijoiden yleisesti kokema toiminnan jatkuvuuden häiriötilanne on meneillään oleva globaali koronaviruspandemia, minkä seurauksena moni organisaatio on joutunut muuttamaan työskentelytapojaan valtaosan työntekijöistä siirtyessä etätöihin. Haastateltavat kertoivat, että pandemia on aiheuttanut organisaatiossa paljon selvittelytyötä. Joissain organisaatiossa oli koettu pandemian alussa haasteita esimerkiksi suojattujen verkkoyhteyksien toiminnan kanssa.

Muita asiantuntijoiden mainitsemia yksittäisiä tapahtumia olivat toimitiloihin liittyvät ongelmat kuten sisäilmaongelma ja tulva, rikoksiin liittyvät kybertapahtumat sekä erään yrityksen tytäryhtiön omistajuuden kaappausyritys. Vakavimmiksi koettiin tilanteet, mitkä on pahantahtoisesti tarkoituksella aiheutettuja. Eräs haastateltava totesi, että vaikka häiriötilanne ei keskeyttäisi koko organisaation toimintaa, se voi aiheuttaa paljon selvittelytyötä ja muutoksia toimintatapoihin. Toimintojen häiriöstä tai täydellisestä keskeytymisestä voi koitua organisaatiolle myös taloudellista haittaa. Häiriötilanteiden aikana asiantuntijat korostivat hyvän yhteistyön ja sujuvan viestinnän tärkeyttä.

JATKUVUUDEN KESKEYTYSTEN EHKÄISY JA RESILIENSSIN VARMISTAMINEN

Jatkuvuus ja resilienssin varmistaminen nousivat toistuvasti esille asiantuntijoiden vastauksista. Harjoitusten tärkeys koko henkilöstölle tai tietylle osalle henkilöstöä häiriötilanteiden varalta nähtiin tärkeänä. Haastateltujen mukaan harjoitusten kautta suunnitelmat, ohjeet ja toteutukset viedään käytäntöön. Harjoituksien kautta syntyy luottamus arkeen ja tekemiseen toimintojen siirtyessä lihasmuistiin. Eräs haastatelluista kuvasi harjoitusten tärkeyden seuraavasti: *"Harjoittelun kautta löytyy prosessin, dokumentaation tai kyvykkyyden osalta kehittämiskohteita."*

Jatkuvuussuunnittelun tavoitteena on turvata organisaation kriittisten prosessien toiminta häiriötilanteissa. Organisaation tulee tuntea oma toimintaympäristönsä, jotta jatkuvuutta voi suunnitella ja toteuttaa kattavasti sekä onnistuneesti. Jos kriittisiä prosessejaan ei tunne, mahdollisuus väärien asioiden turvaamiseen kasvaa. (Valtiovarainministeriö 2016, 27.) Yritysten vapaaehtoinen ja omalähtöinen varautuminen toiminnan jatkuvuuden varmistamiseksi eri tavoin sekä henkilöstön kouluttaminen poikkeavia tilanteita varten toimii yritysten kykynä toimia häiriötilanteissa (Suomi.fi 2021).

> ***Jatkuvuussuunnittelun tavoitteena on turvata organisaation kriittisten prosessien toiminta häiriötilanteissa.***

Haastatteluista nousi esille laitehallinnan ja järjestelmien tunteminen sekä ajantasaisuus. Myös kriittisyysluokittelut nostettiin esille tärkeänä toimenpiteenä. Haastateltujen mukaan niin kriittiset järjestelmät kuin kriittiset henkilöt tulee kahdentaa. Toisin sanoen osaaminen ja järjestelmät eivät saa olla vain yhdessä paikassa tai vain yhden asiantuntijan takana. Asiantuntijat korostivat vastauksissaan myös prosesseja, toiminnan jatkuvuussuunnittelua sekä ohjeistusten ajantasaisuutta, käytettävyyttä ja tärkeyttä. Muutama haastateltu asiantuntija nosti vastauksissaan esiin myös vakuutusten ajantasaisuuden, sidosryhmien ja tukitoimintojen luokittelut ja niiden turvaamisen sekä luotettavuuden.

Haastattelujen perusteella toiminnan keskeytysten vaikutusten minimoimiseksi on havaittu tärkeäksi sekä jatkuvuussuunnitelmat että tilanteiden harjoittelu. Kun suunnitelmat ovat ennalta selkeät ja tilanteita on harjoiteltu, jokainen organisaatiossa tietää miten tilanteen sattuessa tulee toimia, eikä aikaa hukata organisoitumiseen. Tämä on nostettu esille myös kirjallisuudessa. Esimerkiksi Craskin mukaan (2021, 233) pelkkä jatkuvuussuunnitelman olemassaolo ei riitä häiriötilanteen tai kriisin sattuessa, vaan tarvitaan myös siihen liit-

tyvää säännöllistä koulutusta ja harjoittelua. Toiminnan jatkuvuuden varmistamisesta kyberhäiriöiden varalta keskusteltaessa haastateltavat nostivat osin esiin saman tyyppisiä elementtejä.

Asiantuntijoiden näkökulmat voi karkeasti jakaa ennakoivaan toimintaan ja järjestelyihin, häiriön aikaisiin suunnitelmallisiin palautumistoimiin sekä vahinkojen minimoimiseen. Toimittajakumppaneihin kohdistuvat jatkuvuutta varmistavat ja parantavat toimet nousivat esiin yhtenä tärkeänä elementtinä. Ennakoivan toiminnan ja järjestelyiden osalta haastateltavat kertoivat pitävänsä tärkeinä toimina varajärjestelmiä, kahdennuksia ja toimintojen sekä henkilöstön eriyttämistä. Henkilöstön osalta nostettiin esiin tarve tehdä henkilöstön tehtävien ja niiden tärkeyden sekä kriittisyyden etukäteistarkastelu.

Häiriön aikaisten erilaisten toimien osalta yksi haastateltava totesi, että ote ei saa herpaantua, vaikka olisi poikkeustila. Toimittajakumppaneiden tärkeyden nosti esiin useampi haastateltu. Luotettavat IT-kumppanit esimerkiksi varmistavat omalta osaltaan organisaation kyberturvallisuutta. Yksi haastateltava nosti vahvasti esiin sen, että organisaation tulee ottaa toimittajaketju täysin hallintaan ja varmistaa sopimuksin sekä erilaisin määrämuotoisin tarkastuksin kyberturvallisuuden asianmukaisuus. Näissä tarkastuksissa kannattaa hyödyntää erilaisia työkaluja ja esimerkiksi ISO27000 standardiin perustuvia kyselyitä sekä fyysisiä paikallistarkastuksia toimittajan tiloissa.

Kaksi haastateltavaa nosti esiin erilaisten uhkaskenaarioiden tarkastelun tärkeyden. Haastateltavat puhuivat näistä skenaarioista tosin hieman erilaisin sanakääntein puhuen "storylinesta" ja tilannekuvasta, mutta ymmärsimme heidän tarkoittavan uhkaskenaarioita. Organisaation henkilökunnan kouluttamista kyberhäiriöiltä suojautumista vastaan nostettiin myös esiin.

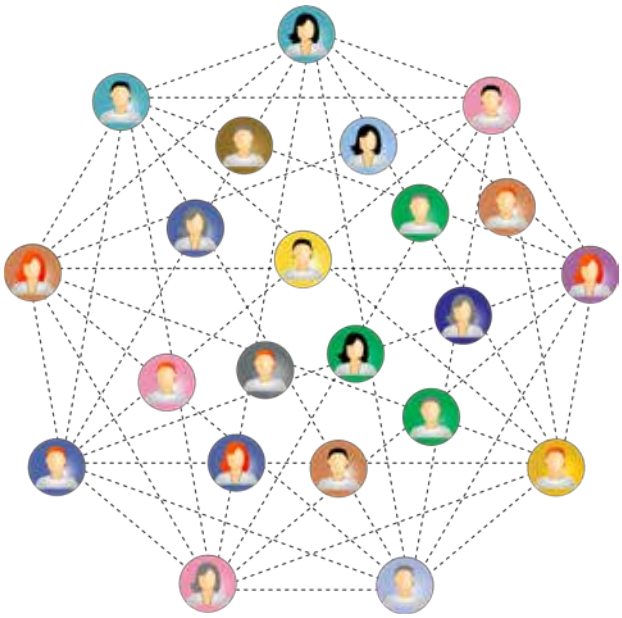
JATKUVUUDENHALLINNAN ULOTTAMINEN TOIMIJAVERKOSTOON

Jos organisaatio ei ota huomioon toimijaverkostoa toiminnan jatkuvuutta suunnitellessaan, altistaa yritys merkittävästi liiketoimintansa häiriöille. Nykyisessä globaalissa toimintaympäristössä riskit eivät enää rajoitu pelkästään paikallisiin toimijoihin, vaan häiriö missä päin maailmaa tahansa voi heijastua organisaatioon. (Crask 2021, 257.) Jatkuvuudenhallintaan kiinnitetään yritysmaailmassa entistä enemmän huomiota. Tähän tarkoitukseen on luotu työkaluja, joista yksi tunnettu on Business Continuity Planning BCP (Hopkin 2018, 203), johon yksi haastatelluistakin nimenomaisesti viittaa kysyttäessä jatkuvuudenhallinnasta toimijaverkostossa.

Ennakoinnilla sekä organisaation yritystoiminnan kokonaisvaltaisesti huomioivalla riskien- ja jatkuvuudenhallinnalla saadaan vähennettyä riskejä. Tehokas riskienhallinta auttaa pitämään yllä organisaation kilpailukykyä samalla, kun se vahvistaa resilienssiä ja operatiivista toimintakykyä. (Buganova, Holla & Moskova 2020.)

Haastateltavilta kysyttiin, kuinka heidän mukaansa resilienssiä ja jatkuvuutta voidaan toimijaverkostossa varmistaa. Vaikka haastateltavia oli edustettuina hyvin erilaisista organisaatioista, näkyi vastauksissa paljon yhteneväisyyttä. Esimerkiksi yhteistyökumppaneiden väliset sopimukset koettiin tärkeäksi.

Yhteistyökumppaneista varmentuminen huomioitiin organisaatioissa erilaisten selvitysten ja tarkastelun avulla, joissa painotettiin luottamusta ja avoimuutta. Paras mahdollinen yhteistyö pohjautuu avoimeen toimintaan, kuten selkeään ohjeistukseen sekä toimivaan viestintään. Näiden lisäksi toimivan yhteistyön pohjalla on hyvin laadittu sopimus. Apuna näissä käytetään muun muassa eri riskianalyysien työkaluja.



Toimijaverkoston keskinäistä luottamusta edesauttaa se, että kaikki osapuolet ovat tietoisia jatkuvuuden suunnitelmasta ja ymmärtävät sen eri osat. Lisäksi on tärkeää, että kaikki osapuolet tietävät mikä heidän roolinsa ja vastuunsa on jatkuvuuden suunnitelman toteuttamisessa. Säännölliset katsaukset suunnitelmaan ja roolien ja vastuiden läpikäyminen tasaisin väliajoin mahdollistavat sen, että jatkuvuuden prosessin toimivuus on varmistettu huolimatta mahdollisista muutoksista organisaatiossa. Työskentely yhteisen tavoitteen eteen motivoi kaikkia osapuolia. (Sterling, Duddridge, Elliot, Conway & Payne 2012, 144-151.)

Haastateltavilta kysyttiin, mitkä seikat he ovat kokeneet tärkeiksi rakennettaessa luottamusta toimijaverkoston kesken. Asiantuntijat korostivat vastauksissa avoimuutta, kommunikointia ja yhteistyötä. Esimerkki avoimuudesta ohjeistuksen jakamisessa: Kun kerrotaan osapuolille mitä ei saa tehdä, niin samassa yhteydessä on hyvä selvittää syyt ja seuraukset mitä voi tapahtua, jos ohjetta ei noudateta. Avoimuuden lisäksi koettiin tärkeäksi selkeä tapa esittää asiat ja tilannetiedon säännöllinen jakaminen, jotta varautumista on mahdollista arvioida yhdessä toimijoiden kesken ajantasaisin tiedoin.

Vastauksissa nousi esiin, että kaikkien toimijaverkostossa on tiedettävä, mitkä ovat kriittiset toiminnot ja toimijat. Asiantuntijat korostivat kommunikoinnissa jatkuvuutta ja monitorointia minkä kautta varmistetaan, että sovitut asiat toteutetaan kuten on luvattu. Luottamuksesta keskusteltaessa eräs asiantuntija nosti esiin Chatham House Rule -käytännön, minkä mukaan kuka tahansa tapaamiseen saapuva saa vapaasti käyttää keskustelusta saatuja tietoja, mutta ei saa paljastaa, kuka on kommentoinut mitäkin. Tämä käytäntö on suunniteltu lisäämään keskustelun avoimuutta. Lisäksi vastaajien kommenteissa tuli esiin, että ennen yhteistyökumppanin valintaa ja yhteistyön aloittamista on tärkeää kerätä tarvittavat tiedot ja vertailla vaihtoehtoja.

JATKUVUUDEN VARMISTAMISTA UHKAAVAT RISKIT SEKÄ TOIMENPIDESUOSITUKSET

Henkilöriskit ovat yksi selvä haastateltujen nimeämä riski toiminnan jatkuvuuden varmistamiseen. Haastateltujen mukaan usein avainosaaminen on yhden henkilön varassa, jolloin vastuualueet kasautuvat hänelle. Tällaisille avainhenkilöille tarvitaan varahenkilö esimerkiksi mahdollisen tapaturman sattuessa. Muita haastateltujen mainitsemia henkilöriskejä ovat sitoutumattomat avainhenkilöt, sidosryhmäverkoston henkilöriskit sekä varsinkin perheyrityksessä omistajien äkillinen poisjäänti päätöksenteosta.

Henkilöriski tarkoittaa henkilöstöstä aiheutuvia riskejä sekä henkilöstöön kohdistuvia riskejä. Jos vastuualueet kasvavat ja varahenkilöä ei ole, avainosaaminen korostuu suuresti. (Suomen riskienhallintayhdistys 2022.) Kristiina Halonen (2013) tutki väitöskirjassaan suomalaisten organisaatioiden ja työterveyshuollon toteuttamaa henkilöriskienhallintaa strategisen johtamisen välineenä. Tuloksissa paljastui kolmeksi merkittävimmäksi henkilöriskeiksi henkinen kuormittuminen, stressi ja työilmapiiri. Henkilöriskit koetaan organisaation toiminnan kannalta merkittäviksi, mutta niitä ei tarkastella paljoakaan osana riskienhallintaa tietämättömyyden ja kompleksisuuden takia. (Halonen 2013, 89, 102, 133.)

> ***Henkilöriski tarkoittaa henkilöstöstä aiheutuvia riskejä sekä henkilöstöön kohdistuvia riskejä.***

Monet muutkin asiat turvallisuuden eri osa-alueilta voivat aiheuttaa riskin toiminnan keskeytymiseen. Haastatteluissa nousi esiin riskejä liittyen kiinteistöihin kohdistuviin väkivaltaisiin tekoihin, tulipaloihin, vesivahinkoihin, sähkökatkoihin, erilaisiin järjestelmähäiriöihin sekä maariskeihin eri maissa ja kaupungeissa. Muutamat haastatellut mainitsivat yksittäisinä nostoina johdolle viestittävän väärän tiedon, jolloin fokus kohdistetaan väärään asiaan. Lisäksi niin sanottu ”mentaalinen blokki” voi estää jatkuvuuden varmistamista.

Organisaation kokonaisvaltaiseen riskienhallintaan sisältyvät myös jatkuvuutta uhkaavat riskit. Riskejä arvioidaan niin ulkoisessa kuin sisäisessäkin toimintaympäristössä. Kriittisiksi luokiteltujen prosessien osalta analysoidaan organisaation omien riskien lisäksi myös sidosryhmien toiminnan riskit. (Valtiovarainministeriö 2016, 35.)

Organisaatiossa saattaa olla vahva näkemys asiasta, joka ei voi tapahtua, jolloin jatkuvuuden varmistamista ei tule tällä kyseisellä alueella tarkasteltua riittävissä määrin. Riskit voivat olla hyvinkin epätodennäköisiä, mutta niitä tulee tarkastella avoimin mielin, koska riskin toteutuessa seuraukset voivat olla hyvinkin suuret.

Toiminnan mukautumiskyvyn parantamiseksi useampi haastateltu toi esille riskitekijöiden tunnistamisen, suunnitelmien teon ja tilanteiden harjoittelun. Hyvä suunnitelma on kirjoitettu ytimekkäästi, se on helposti saatavilla ja informatiivinen (Crask 2021, 215). Tärkeä haastatteluissa esille tullut huomio on, että jatkuvuuden varmistamiseksi resurssointi pitää olla kunnossa jo etukäteen. Ongelmatilanteessa resurssin löytäminen on haastavaa eikä välttämättä toteudu riittävän nopeasti.

JOHTOPÄÄTÖKSET

Kirjallisuuskatsauksen ja haastattelujen perusteella voidaan todeta, että organisaatioiden ja toimintojen erilaisuuden takia jokaisella organisaatiolla tulee olla oma yksilöllisesti analysoitu jatkuvuussuunnitelma. Organisaation tulee itse tunnistaa kriittiset toiminnot ja prosessit, sekä määrittää kokonaisuudet, joihin se tekee jatkuvuuden suunnittelua. Useat eri standardit ja tahot ohjaavat ja määrittelevät liiketoiminnan jatkuvuutta. Ei ole kuitenkaan olemassa yhtä kaikille sopivaa kopioitavaa suunnitelmaa.

Asiantuntijahaastattelujen perusteella kävi ilmi, että kaikki viisi asiantuntijaa mainitsivat samat kolme ilmiötä jatkuvuutta uhkaaviksi tekijöiksi: kyberhyökkäykset, pandemia sekä työntekijöiden virheet. Asiantuntijoiden vastausten perusteella voidaan tulkita, että nämä uhkat ovat riippumattomia organisaation toimialasta. Yllä mainittujen tekijöiden osalta yhteistyö yli oman organisaation rajojen voisi mahdollisesti olla hyödyllistä.

Toimenpidesuositusten osalta voidaan yhteenvetona todeta, että sekä kirjallisuudessa että haastatteluissa tuli selkeästi esille toiminnan jatkuvuuden osalta harjoittelun tärkeys sekä suunnitelmien säännöllinen päivittäminen. Jatkuvuudenhallintaan tulisi osallistaa ihmisiä eri liiketoiminta-alueilta, jotta pystytään varmistamaan eri näkökulmien huomioiminen organisaation sisällä. Organisaation on kuitenkin ymmärrettävä, mikä osa jatkuvuudenhallinnasta on yrityksen vastuulla ja missä menee jakolinja toimivaltaisen viranomaisen vastuulla olevien asioiden osalta.

Lähteet

Buganova, K., Holla, K. & Moskova, E. 2020. Continuity management and risk management as a tool for prevention to origin of crisis situations and increasing the resilience of the enterprise. Economic and Social Development: Book of Proceedings, 127-135. Viitattu 7.4.2022.

Cedergren, A. & Hassel, H. 2022. Using Action Design Research for Developing and Implementing a Method for Risk Assessment and Continuity Management. Safety Science 151. Viitattu 19.03.2022. *https://dx.doi.org/10.1016/j.ssci.2022.105727*

Crask, J. 2021. Business Continuity Management. A Practical Guide to Organizational Resilience and ISO 22301. London: Kogan Page.

Halonen, K. 2013. Pari askelta jäljessä - tuurilla mennään. Tutkimus suomalaisten organisaatioiden ja työterveyshuollon toteuttamasta henkilöriskienhallinnasta strategisen johtamisen välineenä. Tohtori väitöskirja, Aalto yliopisto. Viitattu 26.3.2022. *http://urn.fi/URN:ISBN:978-952-60-5447-6*

Hopkin, P. 2018. Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. Fifth edition. London: Kogan Page.

Huoltovarmuuskeskus 2022. Jatkuvuudenhallinta. Viitattu 23.3.2022. *https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta*

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT -varautuminen. Helsinki: Tietosanoma Oy.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylän ammattikorkeakoulun julkaisuja –sarja.

Klemm, K. & Pajala, K. 2019. Huoltovarmuus: Varautumisella Selviytymiskykyä. Helsinki: Tietosanoma.

Sitra 2022. Resilienssi. Viitattu 23.5.2022. *https://www.sitra.fi/tulevaisuussanasto/resilienssi/*

Suomen Riskienhallintayhdistys. PK-RH-riskienhallinta. Henkilöriskit. Viitattu 26.3.2022. *https://pk-rh.fi/riskien-luokittelu/operatiiviset-riskit/henkiloriskit.html*

Suomi.fi 2021. Poikkeaviin tilanteisiin varautuminen yritystoiminnassa. Viitattu 19.3.2022. *https://www.suomi.fi/yritykselle/muutokset-ja-kriisitilanteet/taloudelliset-vaikeudet/opas/talousvaikeuksien-ennaltaehkaisy/poikkeaviin-tilanteisiin-varautuminen-yritystoiminnassa*

Sterling, S., Duddridge, B., Elliot, A., Conway, M. & Payne, A. 2012. Business continuity for dummies. West Sussex: John Willey & Sons.

Työterveyslaitos 2022. Resilienssi ja jatkuvuudenhallinta. Viitattu 23.5.2022. *https://www.ttl.fi/oppimateriaalit/resilienssi-ja-jatkuvuudenhallinta*

Valtiovarainministeriö 2016. Toiminnan jatkuvuuden hallinta. Viitattu 18.3.2022. *http://urn.fi/URN:ISBN:978-952-251-779-1*

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Viitattu 4.4.2022 *https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_7_2003.pdf*

Julkaisemattomat lähteet

Asiantuntija 1. Teams-haastattelu 21.2.2022. Kotka.

Asiantuntija 2. Teams-haastattelu 25.2.2022. Helsinki.

Asiantuntija 3. Teams- haastattelu 7.3.2022. Helsinki

Asiantuntija 4. Haastattelu 11.3.2022. Helsinki

Asiantuntija 5. Haastattelu 23.2.2022. Helsinki

3 Toiminnan jatkuvuuden varmistaminen julkisissa organisaatioissa

Tommi Linnonmaa, Taina Pekko, Jonas Sjelvgren, Kalle Viitasalo & Sanna Virtaniemi

TOIMINNAN JATKUVUUDEN HALLINTA on julkisissa organisaatioissa ollut tapetilla viimeaikaisten, maailmanlaajuisten tapahtumien vuoksi. Minkälaisia uhkatekijöitä organisaatioiden toimintaan kohdistuu? Miten toiminnan jatkuvuudesta tulisi huolehtia? Mikä on lainsäädännön rooli? Haastattelimme useita eri julkishallinnon organisaatioiden varautumisen ja jatkuvuuden hallinnan asiantuntijoita, joilla on monipuolista kokemusta organisaatioiden toiminnan jatkuvuuden hallinnasta sekä varautumisesta.

TAUSTA

Julkisen sektorin muodostavat valtio ja kunnat. Valtiosektoriin luetaan valtionhallinto, yliopistot, Kansaneläkelaitos, valtion liikelaitokset ja sosiaaliturvarahastot. Kuntiin ja kuntayhtymiin luetaan kunnanhallinto, kunnallinen koululaitos, kuntien ja kuntayhtymien palvelulaitokset ja toimipaikat, jotka eivät ole yhtiömuotoisia, kuten terveyskeskukset, sairaalat, päiväkodit sekä kuntien ja kuntayhtymien liikelaitokset. (Tilastokeskus.)

Julkisen sektorin toimijoilla on lakisääteinen velvoite toimintansa varmistamiselle ja tiettyjen palveluiden tuottamiselle myös poikkeusoloissa. Tästä varautumisen velvoitteesta säädetään valmiuslaissa (1552/2011) (kuva 1). Toiminnan jatkuvuuden varmistaminen on normaaliajan tehtävä organisaation pääasiallisen tarkoituksen ja olemassaolon varmistamiseksi kaikissa tilanteissa.

Julkisten organisaatioiden varautumisvelvoite, valmiuslain (1552/2011) 12 §

Valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa.

Kuva 1. *Valmiuslain 12 §.*

Tässä artikkelissa kuvataan jatkuvuuden hallinnan ja varautumisen keskeisiä käsitteitä, nostetaan yleisellä tasolla esiin joitain jatkuvuuden ja varautumisen julkishallintoon kohdistuvista velvoitteista, muodostetaan näkemys siitä, millaiset seikat ovat olleet tärkeitä organisaatioiden häiriönsietokyvylle sekä millaisia asioita julkishallinnon organisaatioissa erityisesti tulisi huomioida häiriöiden aiheuttamien vaikutusten minimoimiseksi.

Artikkelin tietoperustana on kirjallisten lähteiden lisäksi hyödynnetty kuuden eri julkishallinnon organisaatiossa työskentelevän varautumisen ja jatkuvuudenhallinnan asiantuntijan haastatteluja. Haastateltavilla on monipuolinen tausta ja kokemus toiminnan jatkuvuuden varmistamisesta sekä varautumiseen liittyvistä työtehtävistä. Asiantuntemusta on kertynyt muun muassa Rajavartiolaitokselta, sosiaali- ja terveysalalta sekä tietohallinnosta niin yksityiseltä kuin julkiseltakin sektorilta yhteensä yli 80 vuoden ajalta. Haastattelukysymyksissä ei eritelty normaali- tai poikkeusoloja, vaan varautumista ja jatkuvuussuunnittelua käsiteltiin yleisellä tasolla.

NORMAALIOLOT, HÄIRIÖTILANNE JA POIKKEUSOLOT

Normaalioloiksi katsotaan yhteiskunnan pääsääntöinen tila, jossa elintärkeät toiminnot toimivat normaalisti ja ovat turvattavissa viranomaisten normaalein toimivaltuuksin, eikä niiden turvaamiseksi tarvita valmiuslaissa määriteltyjen viranomaistoimivaltuuksien käyttöönottoa. Poikkeusolot määritellään valmiuslaissa (1552/2011) (kuva 2).

Häiriötilanne määritellään seuraavasti: *"Uhka tai tapahtuma, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. Häiriötilanteita voi esiintyä niin normaalioloissa kuin poikkeusoloissakin."* (Yhteiskunnan turvallisuusstrategia 2017, 97.)

POIKKEUSOLOJEN MÄÄRITELMÄ, VALMIUSLAIN (1552/2011) 3 §

1) Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila;
2) Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii tämän lain mukaisten toimivaltuuksien välitöntä käyttöön ottamista;
3) väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat;
4) erityisen vakava suuronnettomuus ja sen välitön jälkitila; sekä
5) vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti.

Kuva 2. *Valmiuslain 3 §.*

Häiriötilanne voi olla alueellinen tai paikallinen, yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä vaarantava uhka tai tapahtuma. Se voi olla luonnononnettomuus tai ihmisen toiminnasta aiheutuva. Karkeasti häiriötilanteet voidaan jakaa normaaliolojen häiriötilanteisiin ja poikkeusolojen häiriötilanteisiin. Vakava häiriötilanne on poikkeusoloja lievempi tila ja sen hallinta edellyttää toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. (Kokonaisturvallisuuden sanasto 2017, 60.) Häiriötilanteisiin varaudutaan yleisesti jatkuvuussuunnitelmin, valmiussuunnitelmin, koulutuksin, teknisin ja rakenteellisin ratkaisuin sekä harjoittelemalla.

Häiriötilanteet voivat olla hyvin eri pituisia ja vaikutuksiltaan erilaisia. Lyhytaikaisia keskeytyksiä organisaation toimintaan voivat aiheuttaa esimerkiksi tulipalot, niihin liittyvät väärät hälytykset, henkilöstöön tai asiakkaisiin liittyvät seikat, satunnaiset tietoliikenne- tai sähkökatkokset tai vaikkapa sääolosuhteiden muutokset. Haastateltavien kokemusten mukaan tulipalo voi pahimmillaan päättää yhtiön toiminnan sen toimipaikan palaessa ja tuhoisa kyberisku voi aiheuttaa päiviä kestävän katkon tietoliikenteessä, mikä voi nykyaikana vaikuttaa organisaation koko toimintaan. Häiriön lopulliseen laatuun vaikuttaa se, minkälainen organisaatio on kyseessä sekä se, miten erilaisiin häiriöihin on varauduttu.

VARAUTUMINEN ON ENNAKOINTIA JA RISKIENHALLINTAA

Varautuminen on toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen. Varautumistoimenpiteillä voidaan myös varmistaa tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Varautumistoimenpiteitä ovat muun muassa valmiussuunnittelu, jatkuvuudenhallinta, koulutus sekä valmiusharjoitukset. (Kokonaisturvallisuuden sanasto 2017, 15, 69.) *”Laajasti ottaen varautumisena voidaan pitää myös sitä, että lainsäädäntöön sisällytetään esimerkiksi elinkeinoharjoittajille tai kansalaisille velvollisuuksia toimia tietyllä tavalla häiriötilanteissa, tai sitä, että viranomaisille annetaan erityisiä toimivaltuuksia häiriötilanteiden varalta”* (Luoma 2019, 11). Varautumisen prosessi koostuu suunnittelusta ja toiminnasta ja sen tavoitteena on reagoinnin sijaan varautua tulevaan ennalta. (Turvallisuuskomitea.) Haastateltavien mukaan varautuminen on tärkeää keskeytysten vaikutusten minimoimiseksi.

Haastateltavat nostivat esiin ennakoinnin ja harjoittelun merkityksen sekä suunnitelmissa pitäytymisen tärkeyden häiriötilanteessa. Ennakoinnilla tarkoitetaan järjestelmällistä ja osallistavaa prosessia, jossa kerätään ja analysoidaan tietoa. Ennakointityössä laaditaan vaihtoehtoisia kehityskulkuja keskipitkän ja pitkän aikavälin tulevaisuudesta. (Tieteen termipankki.) Ennakoinnin suunnittelu edellyttää erilaisten hiljaisten signaalien havainnointia sekä tutkimustiedon ja ennakointimenetelmien hyödyntämistä odottamattomia tilanteita varten (Turvallisuuskomitea).

Valmiussuunnittelu on normaalioloissa tapahtuvaa varautumisen suunnittelua. Valmiussuunnitelma on valmiussuunnittelun pohjalta syntyvä dokumentti, jota testataan valmiusharjoituksissa. (Kokonaisturvallisuuden sanasto 2017, 38.) Valmiussuunnittelu tukee johtamista häiriötilanteessa ja helpottaa esimiesten työtä sekä resurssien kohdentamista.

Resilienssillä tarkoitetaan organisaation kykyä ylläpitää toimintakykyä muuttuvissa olosuhteissa. Se sisältää myös valmiuden kohdata erilaisia häiriötilanteita ja palautua niistä. Resilienssin taustalla vaikuttaa ajatus siitä, että häiriötilanteet syntyvät odottamattomista tapahtumista. Toimintatapojen tulee olla riittävän

joustavia ja sopeutua ennakoimattomiinkin tilanteisiin, sillä kaikkeen ei voida varautua. (Kokonaisturvallisuuden sanasto 2017, 17.) Resilienssin kannalta merkittävä tekijä on ajantasainen valmiussuunnitelma, jonka tulee olla dynaaminen dokumentti. Dynaamisuus tuo valmiussuunnitelmaan resilienssiajattelun peräänkuuluttamaa joustavuutta.

Riskienhallinta on järjestelmällistä toimintaa ja se sisältää riskien tunnistamisen eli riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. Viranomaisilla on lakisääteinen velvollisuus laatia valmiussuunnitelmia ja riskienhallinta on näiden suunnitelmien olennainen osa. Varautumisessa riskienhallintaa tehdään yhteistyössä useiden eri toimijoiden kanssa. (Kokonaisturvallisuuden sanasto 2017, 50.) Myös haastatellut asiantuntijat totesivat, että riskien tunnistaminen on suunnitelmallista ja järjestelmällistä toimintaa ja luo perustan varautumiselle ja jatkuvuuden hallinnalle. Riskien tunnistamisen prosessien tulisi olla jatkuvia ja niihin tulisi olennaisena osana liittyä toimintaympäristön analysointi.

Haastatteluissa tuli esiin, että organisaatioissa voidaan tunnistaa riskejä, mutta niiden pienentämiseen tai poistamiseen ei välttämättä suunnitella hallintakeinoja. Jos vakavien riskien hallintakeinoja ei suunnitella, voidaan ajautua tilanteeseen, jossa toiminnan jatkuvuus vaarantuu.

TOIMINNAN JATKUVUUTTA UHKAAVIA TEKIJÖITÄ

Sosiaali- ja terveysministeriön (Vuorinen 2019, 13) ohjeessa todetaan, että yksi jatkuvuuden hallinnan tavoitteista on auttaa organisaatiota säilyttämään toimintakykynsä ja samalla minimoida häiriötilanteiden negatiiviset vaikutukset. Organisaation toiminnan jatkuvuutta voivat uhata hyvin moninaiset tekijät. Haastateltavien näkemyksissä nousi esiin kolme eri uhkatekijätyyppiä:

1. Ulkoinen vaikuttaminen
2. Onnettomuudet
3. Ihmisen toiminta

Haastateltavien mukaan ulkopuoliset vaikutteet, kuten maailmantilanne tai erilaiset yhteiskuntarauhan häiriöt, vaikuttavat organisaation jatkuvuuden hallintaan. Esimerkiksi koronaviruspandemialla on ollut organisaatioiden jatkuvuuden hallintaan suuri vaikutus. Tahallista ulkoista vaikuttamista voi olla esimerkiksi jonkin ulkopuolisen, vihamielisen tahon, kuten vieraan valtion tai rikollisen henkilön tai organisaation tarkoituksselliset vaikuttamis- tai vahingoittamistoimet organisaatioon tai sen järjestelmiin.

Myös paikallisen tason uhat, kuten esimerkiksi luonnonmullistukset tai onnettomuudet, on haastateltavien mukaan hyvä tunnistaa. Lisäksi esimerkiksi informaatiovirran häiriöt tai kriittisten tuotantojärjestelmien pidempiaikainen toimimattomuus vaikuttavat haitallisesti organisaation toiminnan jatkuvuuteen.

Kolmantena uhkatekijäryhmänä haastateltavat mainitsevat inhimilliset tekijät. Organisaation työntekijöihin voidaan kohdistaa haitallista vaikuttamista, mikä voi pahimmassa tapauksessa johtaa toiminnan keskeytymiseen. Työntekijä voi huolestuessaan tai väsyneenä jättää jonkin tärkeän vaiheen tekemättä tai toimia epäloogisesti jopa vastoin ohjeita, mikä altistaa virheille. Inhimillistä on myös toimintaympäristön muutosten huomiotta jättäminen tai keskittyminen liiaksi omaan tekemiseen. Haastateltavien mukaan on muistettava, että vaikka virheitä sattuu, niin välinpitämättömyys on vastuuttomuutta, eikä sitä saisi organisaatiossa hyväksyä.

JOHTAMISEN JA HARJOITTELUN MERKITYS SEKÄ HENKILÖSTÖN ROOLI

Toiminnan jatkuvuuden kannalta haastatteluissa tärkeiksi tekijöiksi nousivat johtaminen, ylimmän johdon sitoutuminen ja sovittujen toimintatapojen jalkauttaminen. Johtamisjärjestelmän tulee olla selkeä ja johtamisen vastuiden tulee olla määriteltyinä. Päällekkäiset prosessit luovat ongelmia ja aiheuttavat häiriötilanteissa sekaannuksia.

Mahdollisen priorisoinnin varalta henkilöstölle on hyvä jo ennalta viestiä organisaation ydintehtävät ja strategiset tavoitteet. Haastateltavien mukaan henkilöstön tulee olla valveutunutta, sillä yksikään suunnitelma ei toimi, jos henkilöstö ei ole sisäistänyt omaa rooliaan riittävän laajasti. Henkilöstön tulee tietää, mitä eri tilanteissa tehdään ja mistä lisätietoa on tarvittaessa löydettävissä. Tämän vuoksi sovittuja toimintatapoja tulee harjoitella. Harjoituksissa testataan usein viestinnän tehokkuutta, oikea-aikaisuutta sekä oikeiden henkilöiden tavoittamista rasittamatta mitään yksittäistä viestintäkanavaa liiaksi. Tämä on tärkeää, sillä häiriötilanteessa tulee voida huolehtia myös strategisista ydintehtävistä.

Haastatteluissa nousi esiin, että voidakseen harjoitella erilaisissa tilanteissa toimimista, on häiriötilanteita osattava ennakoida ja toimintaa häiriötilanteissa suunnitella. Harjoittelun tulee olla suunniteltua ja ennalta tiedotettua. Koulutuksina toimivien harjoitusten on koettu ohjaavan suunnitelmallisempien toimintatapojen sisäistämiseen. Häiriö- ja poikkeustilanteessa on tärkeä noudattaa ennalta laadittuja ja harjoiteltuja suunnitelmia. Harjoittelu ja yhdessä toimiminen tulevat esiin myös suomalaisessa kokonaisturvallisuuden mallissa (Yhteiskunnan turvallisuusstrategia 2017, 5).

TOIMINTA HÄIRIÖ- JA KESKEYTYSTILANTEISSA SEKÄ NIIDEN JÄLKEEN

Varautumisesta huolimatta organisaation toiminta voi häiriintyä tai keskeytyä. Keskeytystilanteiden varalle ja jatkuvuuden hallinnan onnistumisen takaamiseksi organisaatiossa tulee tunnistaa ja määritellä kriittiset toiminnot eli ne toiminnot, joiden on tilanteesta ja olosuhteista huolimatta jatkuttava. Näille kriittisille toiminnoille voidaan kohdentaa erilaisia toimenpiteitä, kuten hallintatoimien suunnittelua. (Vahti 2/2016, 29.)

Haastateltavien mukaan toiminnan keskeytyessä on tärkeä pystyä muodostamaan ajantasainen ja reaaliaikainen tilannekuva. Tilannekuvassa kartoitetaan vauriot, vahinkojen laajuus ja tapahtuman mahdolliset jatkoseuraukset. Tältä pohjalta voidaan tehdä päätös ennalta laaditun suunnitelman soveltamisesta tai päätös kehittää kyseiseen tilanteeseen soveltuva vaihtoehtoinen reagointimalli. Valtiovarainministeriön mukaan tilannekuva sisältää kaiken toiminnan kannalta relevantin informaation ja sen avulla voidaan ennakoida sekä pienentää häiriön vaikutuksia (Vahti 2/2016, 51). Lisäksi haastateltavat pitivät tärkeänä, että organisaatiossa on selkeästi kuvattuna tieto siitä, kenelle mistäkin tapauksesta viestitään ja miten.

> ***Toiminnan keskeytyessä on tärkeä pystyä muodostamaan ajantasainen ja reaaliaikainen tilannekuva.***

Toiminnan keskeytyessä haastateltavat pitivät tärkeänä, että organisaatiolla on erilaisia varautumissuunnitelmia tekniikan, henkilöstön, tilojen ja prosessien varalle sekä varamenetelmiä toiminnan jatkuvuuden turvaamiseksi. Tällaisia varamenetelmiä voivat olla esimerkiksi järjestelmien tarvitsemien tietoliikenneyhteyksien kahdentaminen eri operaattoreille, sähkön saatavuuden turvaaminen sekä yhteistyön ylläpitäminen julkishallinnon ja yksityisen sektorin välillä, jotta häiriötilanteessa joitain toimintoja olisi mahdollista korvata toisilla. Lisäksi haastateltavien mukaan toiminnan jatkuvuuden turvaamisessa keskeistä on organisaation osaaminen ja kyvykkyys, mikä edellyttää riittävien resurssien osoittamista toiminnan jatkuvuustyölle. Yhtenä keinona jatkuvuuden turvaamiselle mainittiin henkilösiirrot toisiin tehtäviin tarvittaessa henkilöstöresurssin maksimaaliseksi hyödyntämiseksi.

Häiriötilanteista toipuminen kuuluu kokonaisturvallisuuden hallintaan. Kokonaisturvallisuuden yleisten periaatteiden mukaan ”häiriötilanteista toipumisen suunnittelu pyrkii aiempaa parempaan kriisinsietokykyyn ja valmiuteen” (Yhteiskunnan turvallisuusstrategia 2017, 28). Häiriötilanteesta toipumiseksi organisaatiossa tarvitaan palautumissuunnitelmia, eli harjoiteltuja prosesseja, miten häiriötilasta siirrytään normaalitilaan ja mitä se vaatii (Tepa-termipankki). Palautumissuunnitelmassa kuvataan, miten organisaation toimintakyky saadaan halutussa järjestyksessä palautettua ennalleen häiriön jälkeen.

SOPIMUKSET JATKUVUUDEN HALLINNAN VÄLINEENÄ

Organisaatiot eivät kykene toimimaan täysin itsenäisesti, vaan tarvitsevat ympärilleen eri sidosryhmistä koostuvan verkoston. Sidosryhmiä ovat kaikki ne tahot, joiden kanssa organisaatio on vuorovaikutuksessa, jotka vaikuttavat sen toimintaan ja joihin sen toiminta vaikuttaa (Tieteen termipankki). Tällöin myös organisaation ulkopuolisilla toimijoilla on vaikutusta organisaation jatkuvuuden hallintaan. Organisaatioiden tuleekin haastateltavien mukaan tunnistaa sen kriittisiin toimintoihin liittyvät palveluntuottajat sekä palveluketjut.

Haastateltavien näkemyksissä nousi esiin sopimusten merkitys resilienssin ja jatkuvuuden varmistamisessa. Häiriö- ja poikkeustilanteet organisaation toimintaan vaikuttavien sidosryhmien kanssa tulee huomioida sopimuksin. Vastuut tulee määritellä selkeästi, jotta sopimusosapuolet tietävät omat vastuunsa sekä roolinsa kaikissa tilanteessa. Sopimusten lisäksi organisaatio tarvitsee kokonaisymmärrystä omasta sidosryhmäverkostosta, sen kokoonpanosta ja eri toimijoiden rooleista.

MITEN JATKUVUUDEN HALLINTAA VOIDAAN PARANTAA

Jatkuvuuden hallinnan kehittäminen on säännöllistä toimintaa (Huoltovarmuuskeskus 2022). ISO 22301 -standardi esittelee jatkuvuuden hallinnan kehittämisen työkaluksi PDCA-syklin (Plan, Do, Check, Act). Malli sisältää suunnittelun (plan), toteutuksen (do), arvioinnin (check) ja toiminnan (act). Viimeisessä vaiheessa tehdään tarvittavat korjaukset ja kehittämistoimet, jonka jälkeen palataan takaisin alkuun eli suunnitteluun. (SFS-EN ISO 22301. 2019, 6.)

Haastateltavien mukaan kriisivalmius, kriisinkestävyys ja kriiseistä toipumisen valmius luodaan normaaliolojen aikana, parhaassa tapauksessa kattavaan tietoaineistoon ja laadukkaaseen riskienhallintaan perustuen. Aiemmin mainitut valmiussuunnittelu, kriittisten toimintojen tunnistaminen, riskienhallinta, ennakointi, johtaminen sekä harjoittelu ovat tärkeitä jatkuvuuden hallinnan keinoja. Näiden toimien kriittinen tarkastelu auttaa organisaatiota saavuttamaan paremman jatkuvuuden hallinnan tason. Organisaatiolla on oltava resilienssiä, kyvykkyyttä ylläpitää toimintakykyä muuttuvissa olosuhteissa. Myös erilaiset keskinäisriippuvuudet tulisi tunnistaa osana kriittisten toimintojen jatkuvuuden varmistamista.

On tärkeää, että ylin johto sitoutuu ja tukee jatkuvuuden hallintaa. Johdon on osoitettava riittävät resurssit varautumisen lakisääteisten tehtävien hoitamiseksi sekä organisaation osaamisen ja kyvykkyyden ylläpitämiseksi. Tukea tarvitaan myös sovittujen toimintatapojen jalkauttamisessa sekä niiden noudattamisessa häiriötilanteissa.

Julkisilla organisaatioilla on perinteisesti selkeät prosessit varautumiselle. Useat haastateltavat kuitenkin tunnustivat, ettei sodan uhan pohtimiselle ole vuosiin annettu juurikaan painoarvoa organisaation varautumisessa. Venäjän hyökkäys Ukrainaan on kuitenkin epävakauttanut maailmanpoliittista ilmapiiriä sen verran voimakkaasti, että varautumisen ja jatkuvuuden varmistamisen arviointi ja kehittäminen ovat saaneet julkisissa organisaatioissa merkittävää painoarvoa.

Lähteet

Huoltovarmuuskeskus 2022. Jatkuvuudenhallinta. Viitattu 22.5.2022.
https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta

Kokonaisturvallisuuden sanasto 2017. Helsinki: Sanastokeskus TSK.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Luoma R. 2019. Viranomaisten toimivaltuudet häiriötilanteissa. Oikeusministeriön julkaisuja, selvityksiä ja ohjeita 2019:18. *http://urn.fi/URN:ISBN:978-952-259-756-4*

SFS-EN ISO 22301 -standardi 2019.

TEPA-termipankki. Toipumissuunnitelma. Sanastokeskus. Viitattu 23.5.2022.
https://termipankki.fi/tepa/fi/haku/toipumissuunnitelma

Tieteen termipankki. Nimitys: Sidosryhmä. Viitattu 22.5.2022.
https://tieteentermipankki.fi/wiki/Nimitys:sidosryhm%C3%A4

Tilastokeskus. Käsitteet: Julkinen sektori. Viitattu 08.04.2022.
https://www.stat.fi/meta/kas/julkinen_sektor.html#:~:text=Julkiseen%20sektoriin%20kuuluvat%20valtio%20ja,Kansanel%C3%A4kelaitos%2C%20valtion%20liikelaitokset%20ja%20sosiaaliturvarahastot

Turvallisuuskomitea. Ennakointi ja varautuminen. Viitattu 19.5.2022.
https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ennakointi-ja-varautuminen/

Vahti 2/2016. Toiminnan jatkuvuuden hallinta. Helsinki: Valtionvarainministeriö.
https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf#page=25&zoom=100,0,0

Valmiuslaki 1552/2011. *https://www.finlex.fi/fi/laki/ajantasa/2011/20111552*

Vuorinen, S. (toim.) 2019. Valmius- ja jatkuvuudenhallintasuunnitelma: Ohje sosiaali- ja terveydenhuollon toimijoille. Helsinki: Sosiaali- ja terveysministeriön julkaisuja 2019:10.
http://urn.fi/URN:ISBN:978-952-00-4046-8

Yhteiskunnan turvallisuusstrategia 2017. Valtioneuvoston periaatepäätös 2.11.2017. Helsinki: Turvallisuuskomitea. *https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2017/*

Julkaisemattomat lähteet

Asiantuntija 1. Skype-haastattelu. 13.3.2022. Järvenpää.

Asiantuntija 2. Teams-haastattelu. 10.3.2022. Helsinki

Asiantuntija 3. Haastattelu. 10.3.2022. Espoo.

Asiantuntija 4. Teams-haastattelu 16.2.2022. Helsinki.

Asiantuntija 5. Haastattelu. 12.3.2022. Kokkola.

Asiantuntija 6. Haastattelu. 22.2.2022. Helsinki.

4 Toiminnan jatkuvuus ja sen harjoittelu

Anssi Kuusela

JATKUVUUDEN SUUNNITTELU ON toimintaa, joka jokaisessa organisaatiossa tulisi hallita, ja suunnittelu on syytä tehdä huolella. Tämä on kuitenkin enintään vain puolet työstä, koska osaaminen ja kyvykkyys vastata muuttuviin uhkiin saavutetaan lopulta vain systemaattisella ja riittävällä käytännön harjoittelulla.

JOHDANTO

Uhat ja niiden kohtaamiseen varautuminen ovat nousseet erityisen merkittävään asemaan niin yhteiskunnallisessa toiminnassa kuin yritystenkin toiminnan kannalta. Tietomurrot, kuten esimerkiksi Vastaamon tietovuoto vuonna 2020, useat erilaiset palvelunestohyökkäykset tietoverkoissa ja esimerkiksi vuoden 2019 loppupuolella leviämään lähtenyt pandemia, Covid-19, herättivät monet toimijat vakavasti pohtimaan varautumisen tasoa ja osaamista. Venäjän käynnistämä hyökkäyssota Ukrainaan vuonna 2022 nosti uhkatason laajasti Euroopassa ja jopa globaalisti aivan uudelle tasolle. Oli perusteltua varautua jopa kaikkein pahimpiin uhkiin eli sotaan ja sodan kaltaisiin uhkiin. Keskeisiä kysymyksiä nousi esiin: Mikä on varautumiseni taso – Onko se riittävä? Miten saavutan ja pidän riittävän osaamisen yllä?

Harjoittelun merkitys osaamiselle on tunnustettu pitkään, mutta yllättävän usein toiminnan jatkuvuuden ja varautumisen osalta harjoittelu tuntuu jäävän monissa organisaatioissa tekemättä. Moni, joka on kokenut tilanteen, jossa organisaationsa toiminnan jatkuvuus on joutunut uhatuksi tai siihen on kohdistunut merkittävä realisoitunut uhka. Tämä kertoo epätietoisuudesta toimintavaihtoehdoista ja eri toimintojen keskinäisistä prioriteeteistä sekä toimenpiteiden oikeellisuudesta ja sopivuudesta. Moni kysyy myös toimenpiteiden laki-

perusteita, joita pohditaan suunnitteluvaiheessa ja sisällytetään oikeaoppisesti suunnitelmiin. Silti toimenpiteiden toteuttaminen poikkeavassa tilanteessa, usein paineen alla, on hankalaa ja joskus jopa mahdotonta, jollei niitä myös harjoitella.

Veikko Huovisen luoma henkilöhahmo, Konsta Pylkkänen, Havukka-ahon ajattelija, totesi kaukoviisaudesta, joksi toiminnan jatkuvuuden suunnittelu ja harjoittelu voidaan lukea: "Se on sitä, että asiat ***harkitaan etukäteen*** *ja* ***kuvitellaan tapaus*** *sikseenkin elävästi, että kun se kerran tapahtuu, on reitit selvät. Tätä lajia on harvalle suotu. Jolla sitä on, niin pitäköön hyvänään!"*

Tässä artikkelissa tarkastelen toiminnan jatkuvuuden ja harjoittelun keskinäistä merkitystä empiirisen kokemukseni kautta tukien päätelmiä eri tutkimuksilla, selvityksillä ja ohjeistuksilla, joita olen koonnut perustaksi muun muassa pitämilleni Laurea-ammattikorkeakoulun turvallisuuden ja riskienhallinnan YAMK-tutkinnon asiantuntijaluennoille toiminnan jatkuvuudesta.

Harjoittelun merkitys osaamistason nostamiselle ja säilyttämiselle on kaikessa toiminnassa keskeisen tärkeä asia. Ilman harjoittelua ei voida tuudittautua ajatukseen hyvästä toimintakyvystä, vaikka suunnittelu sinällään olisi tehty miten hyvin. Suunnitelmat realisoituvat käytännöksi vasta harjoittelun kautta, jossa nousujohteisesti perehdytään siihen, mitä toimenpiteitä pitää kulloinkin tehdä ja miten ne saadaan toteutettua. Harjoittelussa korostuvat toistettavuus ja jatkuva kehittyminen. Toisin sanoen harjoituksia on hyvä toteuttaa säännöllisesti siten, että aiemmin tehdyt virheet ja hidastetekijät otetaan opiksi ja harjoitusten välissä suunnittelussa keskitytään poistamaan näitä havaittuja vikoja ja puutteita.

Harjoittelun merkitystä ei vähennä se, minkä osa-alueen tai kokonaisuuden valossa toiminnan jatkuvuutta kehitetään. Harjoitteita voidaan räätälöidä tarpeen ja organisaation kypsyystason mukaisesti, koska oikein mitoitetut harjoitukset parantavat suorituskykyä ja luovat edellytyksiä jatkuvalle kehittämiselle ja kehittymiselle. Lisäksi harjoituksissa on mahdollista tunnistaa suojattavaa asiaa koskevia puutteita ja kehittää myös niitä edelleen. Harjoittelu tukee niin yksinkertaisten suoritteiden parantumista kuin kompleksistenkin asioiden parempaa hallintaa paineenalaisissa tilanteissa.

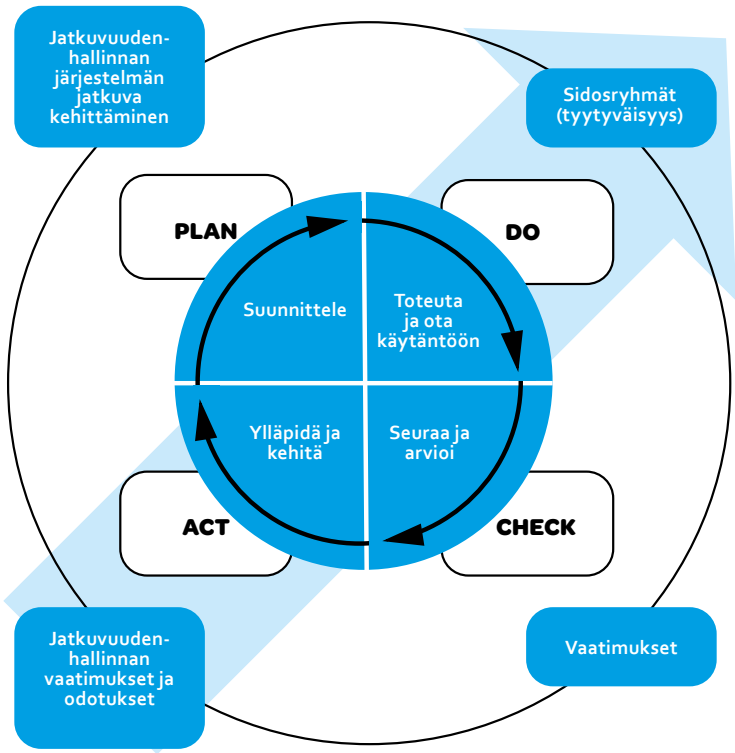
SYSTEMAATTINEN SUUNNITTELU- JA HARJOITUSTOIMINTA TOIMINNAN JATKUVUUDEN TUKENA

Onnistuneen jatkuvuuden hallinnan periaatteet rakentuvat prosessien tuntemuksesta, riittävästä riskianalyysistä ja eri toimintojen välisten riippuvuuksien tuntemuksesta sekä kriittisten järjestelmien tunnistamisesta ja priorisoinnista. Lisäksi pohjalle kannattaa luoda skenaarioita, joita vasten edellä mainitut analyysit ja suunnittelu toteutetaan. (Pietarinen 2018 ja Kuusela 2022.)

Skenaariot ovat tärkeitä ja luovat kehyksen suunnitelmien testaamiselle ja harjaantumiselle niiden toteuttamiseen erilaisissa tilanteissa. Ne tulee laatia sellaisiksi, että ne noudattavat ensisijaisesti riskianalyysin mukaan korkeimman riskiluvun saaneita riskejä. On myös syytä tuottaa sellaisia skenaarioita, jotka harjoitusvaiheessa tuottavat dynaamisesti skaalautuvaa osaamista. Tämä korostuu erityisesti, kun realisoituva riski ei täysin vastaakaan suunnittelun ja harjoittelun skenaariomallia. Esimerkkejä skenaarioista voivat olla mm. seuraavat Valtiokonttorin käyttämät mallit (Pietarinen J. 2018):

- Toimitilat tai merkittävä osa niistä ei ole käytössä
- Henkilöstö, merkittävä osa siitä, ylin johto tai avainhenkilöt eivät ole käytettävissä
- Tietoliikenteen tai -järjestelmien vakavat häiriöt
- Merkittävä palveluntoimittaja, vastapuoli, sidosryhmä tms. ei ole käytettävissä.

Toiminnan jatkuvuuden suunnittelun, kuin suunnitelmien käytännön harjoittelunkin, on hyvä olla systemaattista. Hyvä tapa saavuttaa johdon ja muiden keskeisten toimijoiden hyvä ja jatkuvasti kehittyvä kypsyystaso on pyrkiä toteuttamaan PDCA-mallin mukaista jatkuvan kehittymisen mallia ICT-viitekehyksessä (Kuvio 1). Jatkuvuuden hallinnan standardit, kuten ISO 22301, esittelevät jatkuvuuden hallintajärjestelmän (BCMS, Business Continuity Management System), joka perustuu prosessien jatkuvaan parantamiseen. (Iivari & Laaksonen 2009.) Jatkuvan kehittämisen ja siihen kytketyn harjoitustoiminnan merkitys on suuri laatujärjestelmänäkökulmasta. Muun muassa ISO –standardi määrittelee harjoitustoiminnan merkitystä laatujärjestelmän jatkuvalle kehittämiselle, joka toimii perustana myös toiminnan jatkuvuuden kehittämistä koskevissa osioissa. Tätä kuvataan kuviossa 1.

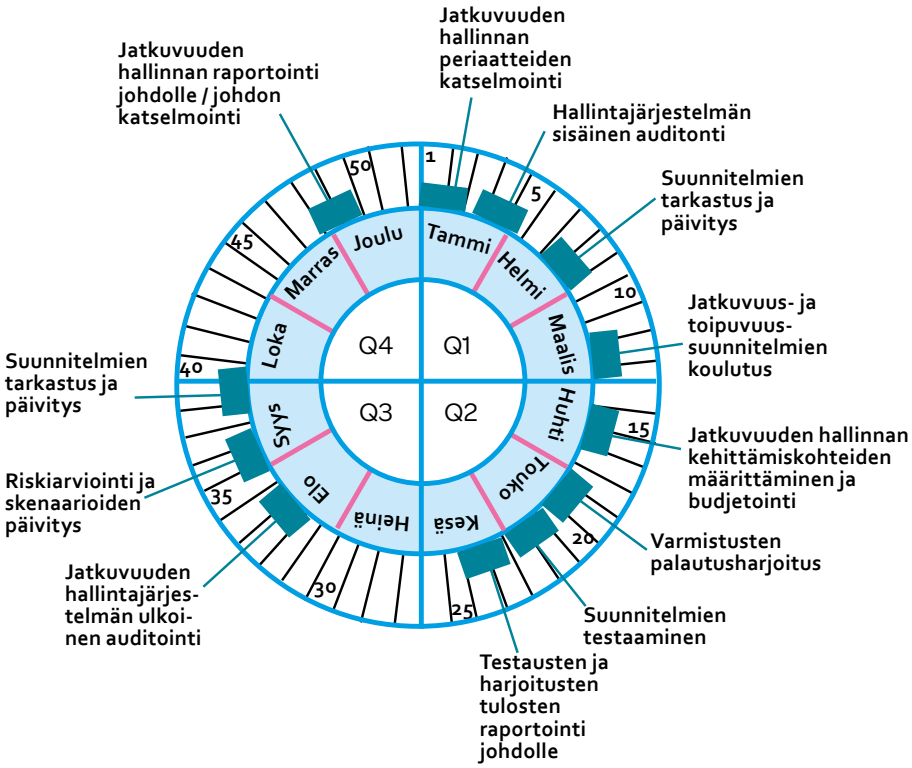


***Kuvio 1**. Jatkuva kehittäminen jatkuvuuden turvaamisen näkökulmasta (mukaellen Iivari & Laaksonen 2009 ja ISO 9001:2008).*

Ensin suunnitellaan (PLAN), sitten toteutetaan (DO), tarkistetaan (CHECK) ja tehdään tarvittaessa korjaukset ja kehitystoimet (ACT). Korjausten jälkeen ympyrässä palataan alkuun eli suunnitteluun. Kehittäminen nähdään spiraalina, päättymättömänä prosessina – jokaisen ympyrän kierroksen jälkeen ollaan kierros lähempänä kulloistakin tavoitetta. Samaa jatkuvan kehittämisen mallia suositellaan käytettäväksi myös muissa tieto- ja kyberturvallisuuden osa-alueissa. (Iivari & Laaksonen 2009.)

Harjoittelu tulee esiin PDCA-mallin vaiheissa DO toteuttaen toimintaa, ja CHECK tarkastetaan toimintaa, jolloin vaiheessa PLAN suunnitellun mukaista toiminnan tasoa ja suunnitelmien toteutuskelpoisuutta testataan skenaariomallin mukaisissa tilanteissa. Samalla tarkastetaan niiden toimivuus ja käyttökelpoisuus ja viedään havainnot edelleen korjaus- ja kehittämistoimenpiteiksi. Tarvittavat ja päätetyt kehitystoimet toteutetaan vaiheessa ACT. Tämän jälkeen palataan taas suunnitteluvaiheeseen PLAN ja päivitetään suunnitelmat. Tämän jälkeen sykli jatkaa pyörimistään suunnitellun kierron mukaisesti.

VAHTI-vaatimustenhallintajärjestelmä on Valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) kehittämä joukko ohjeistuksia, määrityksiä ja vaatimuksia, joiden pohjalle tietojärjestelmät ja prosessit tulee rakentaa, jos halutaan käsitellä valtionhallinnon tietoja. Systemaattisuuden kannalta on tärkeää sitoa toiminnot vuosikelloon. Vahti-ohjeissa (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI, 2016) esitetään esimerkki vuosikelloon kytketystä systemaattisesta toiminnasta, jossa harjoitustoiminta tulee myös esiin (Kuvio 2).



Kuvio 2. *Suunnitelmallisuus jatkuvuudenhallinnassa, vuosikello (VAHTI 2/2016).*

Kun harjoittelu sekä suunnitelmien ylläpito ja päivitys on aikataulutettu jatkuvuuden hallinnan vuosikelloon, on luotu perusta, jonka pohjalta jatkuvuuden hallinnan voi odottaa toimivan erilaisissa muuttuvissa häiriötilanteissa ja muuttuvassa toimintaympäristössä. Kun vielä saadut testaamisen ja harjoittelun tulokset raportoidaan ja palautetaan suunnitelmien ja toimintamallien kehittämiseen, pystytään toiminnan eri vaiheiden vaatimat resurssitarpeet täyttämään. Samalla saadaan mahdolliset virheet korjattua. Säännöllisesti ja systemaattisesti toteutettuna tämä kehittää valmiuksia ja antaa varmuutta toimiin todellisissa erityistilanteissa. Tämä näkyy erityisesti tehtyjen päätösten järkevyydessä ja päätöksentekokyvykkyydessä. (VAHTI 2/2016.) Hyvä suunnittelu ja harjoittelu antavat perustan toiminnalle myös tilanteissa, joissa realisoituva tilanne ei täysin vastaa suunnittelun ja harjoitusten mukaisia tilanteita. Esimerkiksi Myyrmannin kauppakeskuksessa tapahtuneen pommiräjähdyksen yhteydessä sovellettiin johtamisessa Helsinki-Vantaan lentoaseman SAR-suunnitelmaa (Johansson 2002 ja 2004).

Havukka-ahon ajattelija jatkaa: "Mutta tässä lajissa on ***kaksi pahaa vikaa****; asia* ***jää huvikseen tapahtumatta*** *tai se* ***sattuu eri tavalla****. Joka arvaa ottaa nämäkin huomioon, sille on maailmanranta kevyt kiertää."* (Veikko Huovinen: Havukka-ahon ajattelija, 1952.)

HARJOITTELU VS. TOIMINTAYMPÄRISTÖ JA SIDOSRYHMÄT

Toiminnan jatkuvuuden kannalta on tärkeää tunnistaa organisaation toimintaympäristö, niin sisäinen kuin ulkoinenkin. Tämä on hyvä ottaa huomioon kaikissa prosessin vaiheissa sekä myös siinä toimivien eri toimijoiden tarpeet ja merkitys. Säännöllinen harjoittelu yhdessä kriittisten verkostojen kanssa voidaan osoittaa omille sidosryhmille ja kumppaneille oman organisaation kyvykkyyttä turvata oman toiminnan jatkuvuus erityistilanteissa ja kykyyn kohdata mahdolliset ongelmat. Yhdessä harjoittelu on tunnistettu keskinäiseksi luottamusta lisääväksi toiminnaksi. (VAHTI 2/2016 ja HVK 2022).

"Sisäisen toimintaympäristön muodostavat kaikki organisaation sisäiset tekijät, jotka voivat vaikuttaa toimintaan tai tulostavoitteiden saavuttamiseen" (VAHTI 2/2016). Sisäisiä toimijoita arvioitaessa ja kuvattaessa keskeisiä tekijöitä ovat vahtiohjeiden mukaan mm. (VAHTI 2/2016.):

- Hallintotapa, organisaatiorakenne, roolit ja vastuut;
- Toimintaperiaatteet, tavoitteet ja niiden saavuttamiseen tarvittavat strategiat;
- Resursseihin ja tietämykseen liittyvät voimavarat (esim. määrärahat, aika, henkilöt, prosessit, järjestelmät ja teknologia);
- Suhteet sisäisiin sidosryhmiin sekä näiden näkemykset ja arvot;
- Organisaation kulttuuri;
- Tietojärjestelmät, tietovirrat ja päätöksentekoprosessit (sekä muodolliset että epämuodolliset);
- Viraston käyttöön ottamat standardit, ohjeet ja mallit sekä
- Sopimussuhteiden muoto ja laajuus.

"Ulkoisen toimintaympäristön tunnistaminen on tärkeää, jotta voidaan varmistaa, että kansalaisten, asiakkaiden ja muiden ulkoisten sidosryhmien tarpeet ja huolenaiheet otetaan huomioon tavoitteiden asettamisessa ja riskien arvioinnissa" (VAHTI 2/2016). Ulkoista toimintaympäristöä kuvattaessa keskeisiä tekijöitä ovat vahtiohjeiden mukaan mm. (VAHTI 2/2016):

- Hallitusohjelma, Suomen poliittinen ja taloudellinen tilanne
- EU ja globaali ulottuvuus sekä muu kansainvälinen, kansallinen, alueellinen tai paikallinen, yhteiskuntaan, kulttuuriin, politiikkaan, lainsäädäntöön, viranomaismääräyksiin, rahoitukseen, teknologiaan, talouteen, luontoon tai kilpailukykyyn liittyvä toimintaympäristö
- Tietoyhteiskuntaan ja digitalisaatioon liittyvä toimintaympäristö
- Keskeiset organisaation tavoitteisiin vaikuttavat kehityssuunnat yhteiskunnassa; kuten rikollisuustilanne, sabotaasit, terrorismi, onnettomuudet, epidemiat, arvojen muutokset ja polarisoituminen
- Muiden hallinnonalojen toimenpiteet, kuten lainsäädännön ja hallintorakenteiden muutokset
- Suhteet kansalaisiin, asiakkaisiin, rekrytoitavaan henkilöstöön ja kilpaileviin työnantajiin sekä muihin ulkoisiin sidosryhmiin.

Kompleksisuutta menestyksellisen toiminnan jatkuvuuden suunnittelun ja toteuttamisen osalta lisää se, että suunnittelussa ja toiminnassa on osattava ottaa huomioon usein merkittävä määrä ulkoisia sidosryhmiä, joilla voi olla toiminnan kannalta hyvinkin merkittävä rooli organisaatioiden toiminnassa. Sidosryhmiä on hyvä osallistaa suunnitteluun ja harjoitteluun aktiivisesti, jotta voidaan varmistua myös kriittisten sidosryhmien kyvykkyyksistä eritasoissa erityistilanteissa. On myös mahdollista, että sidosryhmät esittävät vaatimuksia organisaation suuntaan. Kyse on suunnittelun ja yhteisen harjoittelun lisäksi myös jatkuvasta vuoropuhelusta organisaatioiden kesken. (VAHTI 2/2016.) Kuviossa 3 on esitetty esimerkkejä sidosryhmistä.

Kuvio 3. *Esimerkki sidosryhmistä, jotka toiminnan jatkuvuuden suunnittelussa ja harjoitustoiminnassa tulee ottaa huomioon (VAHTI 2/2016).*

Organisaation toimintaympäristössä vaikuttavien toimijoiden (sisäisten ja ulkoisten) roolia kannattaa tarkastella ydintoimintojen ja prosessien näkökulmasta. On hyvä pyrkiä yhteistyössä luomaan toimintavalmius, joka takaa toimintakyvyn ja toiminnan jatkuvuuden haastavissakin erityistilanteissa. On tärkeää tunnistaa ne yhteiset kriittiset toiminnalliset kohdat, joissa toiminnan jatkaminen ei esimerkiksi hetkellisesti ole mahdollista. Tällöin toimijoiden on hyvä yhdessä suunnitella, miten tilanteesta toivutaan ja laadittava toipumissuunnitelma myös näiden tilanteiden varalle. Esimerkiksi palvelutoimittajien kanssa on erilaiset vaatimukset huomioitava proaktiivisesti palvelutasosta sovittaessa ja laadittava tarvittaessa eri skenaarioihin soveltuvat palvelutasot / SLA:t (Service Level Agreement). Nämä SLA-vaatimukset on syytä sopia ja dokumentoida selvästi sekä harjoittelussa käydä läpi yhdessä sidosryhmän edustajien kanssa, jotta niiden osalta ei muodostu harhakuvaa toimivuudesta pelkän suunnitelman pohjalta. (VAHTI 2/2016.)

"Hyviä käytänteitä jaetaan ja opitaan harjoittelemalla", todetaan huoltovarmuuskeskuksen toimesta. Tämä linja näkyy huoltovarmuuskeskuksen ja sen alaisten poolien järjestämissä harjoituksissa sekä sen niin sanotusti sponsoroimassa muussa harjoitustoiminnassa. HVK korostaa ohjeistuksessaan jatkuvuudenhallinnan merkitystä erilaisista toiminnan katkoksista aiheutuvien häiriöiden kustannusvaikutusten vähenemistä, kun se toteutetaan järjestelmällisesti ja säännöllisesti. Harjoittelun merkitys korostuu ohjeistuksessa ja se nähdään juuri sinä keinona, jolla osaaminen ja toimivuus saavutetaan ja jatkuvan kehittymisen polku turvataan yhteistyössä kaikkien sidosryhmien kanssa verkostomaisesti. (HVK 2022.)

Testaaminen, harjoittelu ja koulutus oppimisen ja kehittämisen kulmakivinä tähtäävät jatkuvuutta ja toipumista ohjaavien ryhmien perehdytykseen. Lisäksi tavoitteena on saattaa kaikki muut suunnitelmien kanssa tekemisissä olevat tahot tietoisiksi toimenpidevelvoitteistaan, vastuistaan sekä rooleistaan. Näin luodaan näyttöpohjainen kuva toimijoiden kyvykkyydestä häiriötilanteen ratkaisemisessa ja toiminnan jatkuvuuden turvaamisesta toipumissuunnitelmia myöten ja varmistetaan, että suunnitelmissa on otettu huomioon kaikki ydintoimintojen jatkuvuus ja toipuminen. (VAHTI 2/2016.)

ESIMERKKEJÄ HARJOITTELUSTA

Toiminnan jatkuvuussuunnittelu ja siihen liittyvä harjoittelu on lisääntynyt eri organisaatioissa varsin nopeasti viimeisenä noin kymmenenä vuotena. Kun aiemmin harjoittelu koettiin lähinnä viranomaisorganisaatioiden harjoittamiksi varsin suljetuiksi tilaisuuksiksi, joihin ei ympäröivällä yhteiskunnalla ja monilla sidosryhmillä ollut juuri minkäänlaista näkymää, on harjoitustoiminta muuttunut osallistavammaksi sidosryhmien suhteen ja toimintaympäristön merkitys on laajasti ymmärretty.

Harjoituksiin liittyy nykyisin jonkinlainen tilanteiden simulointi, jonka avulla luodaan mahdollisimman todentuntuinen tilanne ja tapahtumaympäristö harjoittelevalle joukolle. Tarkkailijat seuraavat eri ryhmien ja toimijoiden toimintaa ja tilannekuvauksiin haetaan elävyyttä usein yhdistämällä virtuaalista ympäristöä ja sähköisiä medioita sekä oikeita maalihenkilöitä. Harjoitukset ovat pienimuotoisista pienen ryhmän pöytä- / desk-top -harjoituksista aina laajoihin, jopa tuhansien henkilöiden harjoituksiin. Yksittäisen organisaation kannalta usein tärkeimpiä ja kehittävimpiä ovat omat keskeisiin kehittämistarpeisiin keskittyvät harjoitukset. Keskeistä on, että toimintaa toteutetaan tilanteeseen eläytyen ja sitä arvioidaan reaaliaikaisesti jatkuvasti riittävällä tarkkailijavoimalla.

Esimerkiksi Laureassa, kuten useassa muussakin korkeakoulussa, harjoittelu on integroitu osaksi suunnittelun vuosikelloa kokonaisprosessin rakentuessa riskilähtöiseen ajatteluun, analyyttisuuteen, suunnitelmallisuuteen ja ennen kaikkea harjoitteluun, josta saadut havainnot palautetaan jatkuvan kehittämisen tueksi. Arviointi toteutetaan ulkoisten arvioitsijoiden lisäksi myös vahvalla itsereflektiolla. Vastaavaa on alettu toteuttaa useiden yritysten ja muiden toimijoiden toimesta. Ulkoinen arvioija on usein myös jossain määrin vertainen, jolloin tätä voidaan toteuttaa koulujen välisesti ristiin pölyttäen ja resursseja lainaten. Simulointiin panostetaan tilanteesta ja vaatimustasosta riippuen paljonkin. Toisaalta tilannekuvauksia voidaan tehdä myös puheella, videoilla, kirjallisilla kuvauksilla ja perinteisellä esitystekniikalla.

Monet toimijat ovat mieltäneet myös ulkoa ostetun konsultoinnin liian arvokkaana ja tällöin oppilaitoksilta, erityisesti Laurean kaltaisilta turvallisuuden ja riskienhallinnan tutkintoa kouluttavilla oppilaitoksilla on erityinen mahdollisuus toimia toimintana jatkuvuutta kehittävän organisaation kehittämiskumppanina.

LOPPUSANAT

Havukka-ahon ajattelija muistuttaa kuinka lopuksi kannattaa muistaa se, että kenellä on jatkuvuuden hallinta ja sen edellyttämä osaaminen kunnossa ei tarvitse jälkiviisastella: "Kaikista paras ja imelin viisauvenlaji on jälkiviisaus, sillä alalla saahaan eniten aikaan. Siinä on tapaus mennyttä aikakautta, mutta se kuvitellaan esiin tulevaksi ja sakilla setvitään, miten olisi parasta käyttäytyä. Tässä lajissa on ihminen viisaimmillaan. Jälkiviisaan silmä on somassa paikassa, se kahtoo taaksepäin. (Veikko Huovinen: Havukka-ahon ajattelija, 1952.)

Lähteet

Huoltovarmuuskeskus. Jatkuvuudenhallinta. Viitattu 31.5.2022. *https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta*

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki: Tietosanoma.

ISO 9001:2008. Quality management systems

Vahti 2/2016. Toiminnan jatkuvuuden hallinta. Helsinki: Valtionvarainministeriö. Viitattu 31.5.2022. *https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf#page=25&zoom=100,0,0*

Julkaisemattomat lähteet

Keskustelut johtamisesta Myyrmannin kauppakeskuksen pommiräjähdyksen (2002) yhteydessä, pelastustoiminnan johtajana toiminut Leif Johansson ja Anssi Kuusela (2002 ja 2004).

Kuusela, A. 2022. Toiminnan jatkuvuuden turvaaminen ja sen harjoittelu. Asiantuntijaluento 2.4.2022, Laurea-ammattikorkeakoulu.

Pietarinen, J. 2018. Toiminnan jatkuvuus -käytännön näkökulma. Seminaariesitys 14.3.2018, Valtiokonttori, Helsinki.

5 Virka-apu viranomaisten operatiivisen toiminnan jatkuvuuden varmistajana

Miika Aholainen, Saija Hertteli, Pia Hurme, Jaakko Lyytikäinen & Mika Suutarinen

VIRANOMAISTEN VÄLINEN VIRKA-APUYHTEISTYÖ on monialaista toimintaa, kuten artikkelia varten tehdyistä viranomaishaastatteluista selviää. Viranomaisen toiselle antama virka-apu liittyy muun muassa pelastustoimintaan, turvallisuuden varmistamiseen sekä avunantoon. Yhdessä tehden luodaan vankkaa pohjaa viranomaisten väliselle yhteistyölle.

JOHDANTO

Viranomaisten operatiivisen toiminnan jatkuvuus varmennetaan tarvittaessa viranomaisyhteistyöllä ja virka-avulla. Tässä artikkelissa tarkastellaan Laurea-ammattikorkeakoulun ja viranomaisorganisaatioista kootun asiantuntijaryhmän yhteistyönä virka-apua viranomaisten toiminnan jatkuvuuden varmistajana. Tarkasteltavina esimerkkikohdeorganisaatioina ja toimijoina käytetään Poliisia, Tullia, Puolustusvoimia, ensihoitoa, pelastustoimea sekä sosiaalitoimea, jotka kirjoittajien kokemusten perusteella yleisesti osallistuvat toisen viranomaisen tukemiseen joko yhteistoiminta- tai virka-apuperusteisesti. Artikkeli perustuu nimettyjen organisaatioiden edustajille artikkelia varten tehtyihin haastatteluihin sekä aiemmin julkaistuihin haastatteluihin. Tausta-aineistona on hyödynnetty virka-apua ja viranomaisyhteistyötä määrittelevää kansallista lainsäädäntöä.

Virka-apua voidaan lakiperusteisesti pyytää ja antaa niissä nimenomaisissa tilanteissa, joissa toimivaltaisen viranomaisen omat resurssit tai kyvykkyydet eivät riitä tilanteen ratkaisemiseen. Esimerkkeinä viranomaisten yhteistyötä edellyttävästä tilanteesta voivat olla laaja liikenneonnettomuus, suuri ja pitkäkestoinen tulipalo tai esimerkiksi räjähdeuhka.

VIRANOMAISTEN OPERATIIVISEN TOIMINNAN JATKUVUUDEN PERUSTEET

Viranomaisten välinen yhteistyö ja virka-apu pohjautuvat kaikkien viranomaisten toimintaa ohjaavaan hallintolakiin (434/2003). Hallintolain yhtenä hyvän hallinnon perusteena on se, että viranomaisen on toimivaltansa rajoissa avustettava toista viranomaista hallintotehtävän hoitamisessa. Viranomaisten välisestä yhteistoiminnasta ja virka-avusta säädetään erikseen kunkin viranomaisen toimintaa ohjaavassa lainsäädännössä. Lisäksi esimerkiksi Poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta on säädetty oma laki (687/2009). Tämän niin sanotun PTR-lain tarkoituksena on edistää edellä mainittujen turvallisuusviranomaisten välistä yhteistoimintaa. Samoin esimerkiksi Puolustusvoimien virka-avusta Poliisille on annettu oma lakinsa (781/1980).

Kaikki viranomaisten välinen yhteistyö ei kuitenkaan ole virka-apuperusteista, vaan sitä toteutetaan myös toimivaltaisen viranomaisen koordinoimana muiden viranomaisten kanssa, joilla on lakisääteisten tehtäviensä puolesta velvoite tai valtuutus toimintaan osallistumiseen. Osa näiden tehtävien puitteissa tehtävästä viranomaisyhteistoiminnasta perustuu viranomaisten tai niiden alaisten laitosten välisiin yhteistoimintasopimuksiin tai -muistioihin (Pelastustoiminnan palveluyksikön Palopäällikkö 2022). Näissä tilanteissa yhteistoimintaa kutsutaan usein pelkistetysti viranomaisyhteistyöksi, ilman virka-apuvelvoitetta ja -menettelyä. (Valtonen, 2010, 25). Esimerkiksi pelastustoimintaan liittyen Pelastuslaki (379/2011) velvoittaa useita viranomaisia osallistumaan pelastustoimintaan ja viranomaisyhteistoimintaan ilman, että kyseessä on varsinainen virka-apu.

Viranomaisyhteistoimintaa pelastustoiminnassa säätelee Pelastuslain (379/2011) 46 §, jonka mukaan valtion ja kunnan viranomaiset ovat pelastuslaitoksen johdolla velvollisia toimimaan onnettomuus- ja vaaratilanteissa niin, että pelastustoiminta voidaan toteuttaa tehokkaasti. Kyseinen laki säätää pelastustoiminnan kannalta keskeisimpien viranomaisten, kuten hätäkeskuksen, Puolustusvoimien, Rajavartiolaitoksen, Poliisin sekä sosiaali- ja terveysviranomaisten tehtävistä pelastustoiminnassa. Näin ollen pelastusviranomainen ei joudu juuri koskaan pyytämään varsinaista virka-apua, vaan sen edustajat velvoittavat muita toimijoita osallistumaan varautumisen suunnitteluun, tai käskevät niitä osallistumaan käytännön pelastustoimintaan (Pelastuslaki 379/2011, 46 §; Tilanne- ja johtokeskuksen Palopäällikkö 2022).

Viranomaisten varautumisesta säädetään valmiuslain (1552/2011) 12 §:ssä, joka velvoittaa valmiussuunnitelmin ja muilla toimenpiteillä varmistamaan tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Valtioneuvoston periaatepäätös yhteiskunnan turvallisuusstrategiasta (2017, 7) ohjaa yleisellä tasolla kokonaisturvallisuuden yhteistoimintaa viranomaisten ja muiden toimijoiden välillä. Häiriötilanteella tarkoitetaan uhkaa tai tapahtumaa, joka vaarantaa yhteiskunnan elintärkeitä toimintoja ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista tiiviimpää tai laajempaa yhteistoimintaa (Sisäministeriö 2019, 22).

ESIMERKKEJÄ VIRKA-AVUN TARPEESTA OPERATIIVISEN TOIMINNAN TURVAAMISESSA

Artikkelia varten tehtyjen viranomaisten edustajien haastattelujen perusteella virka-apu liittyy hyvin usein akuutteihin tilanteisiin. Yleisenä havaintona voidaan todeta, että viranomaiset toimivat haastattelujen perusteella lainsäädännön mukaisesti siten, että virka-apua pyydetään ensisijaisesti silloin, kun toimivaltaisen viranomaisen omat kyvykkyydet, kuten henkilöstö- tai kalustoresurssit, eivät ole tehtävän hoitamiseen yksinään riittävät. Virka-apumenettelyllä ja useamman kuin yhden viranomaisen osallistumisella tehtävään tällöin varmistetaan, että toimivaltaisen viranomaisen vastuulla oleva tehtävä saadaan omista suorituskykypuutteista huolimatta toteutettua ja toiminnan jatkuvuus varmistettua. Poliisin rooli virka-apua vastaanottavana tai toteuttavana toimijana on artikkelia varten tehtyjen haastattelujen perusteella erityisen keskeinen. Poliisin toimiessa virka-apua antavassa roolissa, on sen tehtävänä usein toisen viranomaisen toiminnan turvaaminen.

> ***Virka-apua pyydetään ensisijaisesti silloin, kun toimivaltaisen viranomaisen omat kyvykkyydet, kuten henkilöstö- tai kalustoresurssit, eivät ole tehtävän hoitamiseen yksinään riittävät.***

Sekä ensihoidon että sosiaalitoimen pyytämä virka-apu liittyy useissa tapauksissa poliisin tuen pyytämiseen. Poliisia tarvitaan joko suojaamaan ensihoidon tai sosiaalitoimen henkilöstön toimintaa, tai vaihtoehtoisesti poliisia tarvitaan käyttämään toimivallassaan olevia pakkokeinoja tuettavan viranomaisen tehtävän suorittamisen tukemiseksi. Lisäksi poliisi voi tukea näitä toimijoita henkilöiden etsintään ja paikantamiseen soveltuvilla suorituskyvyillä, kuten miehittämättömillä ilma-aluksilla.

Haastatellun ensihoidon edustajan mukaan raja hätäkeskuksen määrittämän hälytystehtävän ja varsinaisen virka-avun välillä on kuitenkin usein epäselvä (Sairaanhoitopiirin ensihoidon kenttäjohtaja, 2022). Myös sosiaalitoimen edustajan mukaan poliisin kanssa tehtävän yhteistoiminnan tehtävät tulevat pääsääntöisesti hätäkeskuksen kautta (Sosiaalitoimen lapsiperhetyön päällikkö, 2022), eikä tällöin ole välttämättä kyse muodollisesti pyydetystä virka-avusta vaan normaalista hälytystehtävään liittyvästä yhteistoiminnasta tilanteessa, joka koskettaa useita viranomaisia ja näiden vastuualueita.

Sosiaalitoimen näkökulmasta poliisin antamaa virka-apua pyydetään erityisesti silloin, kun kotikäyntiin liittyvällä tehtävällä tulee tietoon väkivallan uhkaa (Sosiaalitoimen lapsiperhetyön päällikkö, 2022). Poliisin näkökulma yhteistoimintaan ensihoidon ja sosiaalitoimen kanssa tehtävästä yhteistoiminnasta yhtenee edellisiin näkökulmiin. Poliisin havaintojen mukaan sosiaalitoimen kanssa tehtävästä yhteistoiminnasta yleisiä ovat erityisesti lasten ja nuorten kiireellisiä huostaanottoja ja sijoittamisia koskevat tehtävät, sekä karanneita nuoria ja alaikäisten asuin- ja elinolojen tarkastuksia koskevat tehtävät. Poliisin apua tarvitaan lisäksi tilanteissa, joissa terveydenhuollon edustajat pyytävät mielenterveyspotilaisiin liittyvää virka-apua, esimerkiksi kun potilas ei suostu ambulanssin kyytiin tai joutuu tahdosta riippumattomaan hoitoon. (Valvonta- ja hälytyssektorin komisario, 2022). Myös pelastustoimen osalta yksi yleinen virka-aputehtävän tarve liittyy oman toiminnan turvaamiseen. Pelastustoimen osalta pyyntö poliisin virka-avusta voi kohdistua esimerkiksi palotarkastajan työn turvaamiseen (Tilanne- ja johtokeskuksen Palopäällikkö 2022).

Pelastustoimen tukemisen osalta on huomattava, että vaikka pelastuslaitos saakin usein tukea muilta viranomaisilta pelastustehtävän hoitamiseen, ei tällöin ole kuitenkaan välttämättä kyse varsinaisesta virka-avusta, vaan lakisääteisestä pelastustoimintaan osallistumisesta. Pelastustoimen tukeminen perustuu edellä kuvatusti pelastuslain 46 §:än, joka määrittelee eri toimijoille ja viranomaisille velvoitteen osallistua pelastustoimintaan toimintaa johtavan pelastustoimen johtajan käskystä (Tilanne- ja johtokeskuksen Palopäällikkö 2022).

Pelastustoimen osalta varsinainen virka-apua edellyttävä tapahtuma voisi liittyä CBRN-uhkaan (kemiallista, biologista tai radiologista uhkaa sisältävä tilanne), jolloin voi syntyä tilanne, että pelastuslaitoksen työvuorossa olevan henkilöstön ammattitaito loppuu kesken. Tällöin apua voidaan pyytää esimerkiksi Puolustusvoimilta, jolla on tällaisiin tilanteisiin enemmän erityiskalustoa ja -osaamista. Näissäkin tilanteissa pelastustoiminnan johtajalla on kyky kokonaistilanteen johtamiseen, vahinkojen rajoittamisen käynnistämiseen ja oman toiminnan suojaamiseen, mutta tilanteen tarkoituksenmukainen ratkaisu edellyttää useamman viranomaisen toisiaan tukevaa yhteistoimintaa (Pelastustoiminnan palveluyksikön Palopäällikkö, 2022).

VIRKA-AVUN MUOTOJA

Eri viranomaiset antavat virka-apua sekä henkilöstöresursseina että kaluston muodossa. Henkilöstöresurssit voivat olla a) erityiskoulutettua henkilöstöä kuten esimerkiksi räjähteiden raivaamiseen koulutettua henkilöstöä, kun Poliisi pyytää siihen virka-apua Puolustusvoimilta, b) toimivaltaista henkilöstöä, kun esimerkiksi sosiaalitoimen kotikäynnille mahdollisen väkivallan uhan takia pyydetään poliisia turvaamaan tehtävää tai c) lukumääräistä henkilöstöä, esimerkiksi Puolustusvoimien virka-apumuodostelmien käyttö alueen eristämiseen tai henkilöstön etsimiseen. Kalustoresurssit voivat olla erityiskalustoa, kuten miehittämättömiä ilma-aluksia, eli droneja alueen valvomiseksi tai henkilön etsimiseksi, tai esimerkiksi edellä mainittuihin räjähteiden raivaamiseen soveltuvaa kalustoa.

Pelastuslaitoksen kalustollista suorituskykyä on käytetty tukemaan poliisia esimerkiksi tarvittaessa pääsyä korkealle tai tilanteen edellyttäessä raskasta murtovälinekykyä. Pelastusviranomainen voi tukea poliisia esimerkiksi nostolavalla tai vastaavalla kurottamiskalustolla poistettaessa henkilöä korkealta. Lisäksi pelastuslaitoksen murtovälineitä tai raivauskalustoa voidaan hyödyntää esimerkiksi tilanteessa, jossa itsensä johonkin kohteeseen kahlinneita henkilöitä joudutaan irrottamaan esimerkiksi teräsketjuista. (Tilanne- ja johtokeskuksen Palopäällikkö 2022). Lisäksi pelastustoimi voi tukea esimerkiksi ensihoitoa antamalla kiireellistä kantoapua tai vaikka venekuljetusta (Tilanne- ja johtokeskuksen Palopäällikkö 2022).

Myös Poliisi voi olla edellä kuvatun pelastustoiminnan antaman tuen mukaisesti virka-apua pyytävä ja vastaanottava viranomainen. Poliisi voi joutua itse pyytämään virka-apua myös muissa vaativissa tilanteissa, joissa sillä ei itsellään ole tarvittavaa osaamista, kalustoa tai muuta välineistöä tehtävän hoitamiseen. Vaativissa tai erityistilanteissa, joissa on henkeen tai terveyteen kohdistuva uhka, voidaan apua pyytää pelastustoimen ja ensihoidon lisäksi Puolustusvoimilta. (Valvonta- ja hälytyssektorin komisario 2022; Laki puolustusvoimien virka-avusta poliisille 781/1980, 1 ja 2§).

Puolustusvoimat valmistautuu antamaan virka-apua ensisijaisesti poliisille tai pelastuslaitokselle yhteiskunnan turvaamiseksi, järjestyksen ylläpitämiseksi ja terrorismirikosten estämiseksi. Käytännön tasolla Puolustusvoimat toteuttaa vuosittain useita satoja virka-aputehtäviä. Näistä pääosa perustuu poliisin ilmoituksiin sotilasräjähteestä ja virka-apupyyntöihin niiden raivaamiseksi. Nämä tehtävät eivät välttämättä aina täytä virka-aputehtävän määritelmää, vaan niitä toteutetaan Puolustusvoimien lakisääteisen tehtävän puitteissa.

Mikäli räjähdetilanteeseen liittyy uhka hengelle, terveydelle tai ympäristölle, on yleisen järjestyksen ja turvallisuuden turvaamisen johtovastuu poliisilla, jolloin virka-apumenettelyn käyttö tuen saamiseksi on perusteltua. Räjähteiden raivaamisen lisäksi Puolustusvoimia ja sen johdossa olevia suorituskykyjä voidaan käyttää esimerkiksi alueen eristämiseen ja henkilöiden etsimiseen. Erityisesti Puolustusvoimien virka-apua voidaan käyttää silloin, kun viranomaisen tukitehtävään tarvitaan nopeasti paljon henkilöstöä, erikoiskoulutettua henkilöstöä tai erikoiskalustoa. (Puolustusvoimat 2022; Luukkola 2021; Laki Puolustusvoimien virka-avusta poliisille 781/1980, 1 ja 2 §).

Myös Tulli joutuu lakisääteisten tehtäviensä toteuttamisessa tukeutumaan virka-apuun. Tehtäviensä luonteen vuoksi Tulli pyytää virka-apua ajoittain myös ulkomaisilta viranomaisilta, sekä tarvittaessa antaa virka-apua ulkomaisille viranomaisille. Kotimaisten viranomaisten kanssa yhteistoiminta keskittyy niin sanotusti PTR-yhteistyöhön, joka on poliisin, Tullin ja Rajavartiolaitoksen yhteistoimintaa. (Tullin valvontapäällikkö, 2022; Tullilaki 304/2016, 76 §; Laki poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta 687/2009 1 §).

PTR-yhteistoiminnasta on huomattava, että myös sitä tehdään lakisääteisesti muutoinkin kuin virka-apuperusteisesti. PTR-laki antaa näille viranomaisille laajan toimivallan toimia toisen viranomaisen rikostorjunnan toimivaltaan kuuluvalla alueella. PTR-viranomainen voi pyynnöstä suorittaa toisen PTR-viranomaisen puolesta tämän tehtäväalueeseen kuuluvan yksittäisen rikostorjuntaan liittyvän toimenpiteen käyttäen niitä toimivaltuuksia, joita se saa käyttää omalla tehtäväalueellaan sille kuuluvissa rikostorjuntatehtävissä (Laki poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta 687/2009 1 §).

VIRKA-AVUN ANTAMISEEN LIITTYVIÄ RAJOITTEITA

Kaikkiin virka-apupyyntöihin ei voida vastata myöntävästi. Virka-apupyynnöstä voidaan kuitenkin kieltäytyä lähtökohtaisesti vain, mikäli pyydettyä resurssia ei ole tai sen luovuttaminen toiseen käyttöön vakavasti vaikuttaa oman lakisääteisen tehtävän suorittamiseen. Tällaisissa tilanteissa edellytyksenä on usein, että meneillään on oma kiireellinen tehtävä, jossa pyydetty resurssi on jo käytössä (Tilanne- ja johtokeskuksen Palopäällikkö 2022, Ensihoidon kenttäjohtaja 2022). Myöskään kaikkiin pyydettyihin (ensihoidollisiin) ei-kiireellisiin varautumistehtäviin ei pystytä vastaamaan virka-avun muodossa. Tällainen tehtävä saattaa luonteensa puolesta kuulua esimerkiksi kaupalliselle toimijalle (Ensihoidon kenttäjohtaja 2022).

Haastatteluihin osallistuneet viranomaisten edustajat totesivat yhtenäisesti, että virka-apua ei yksiselitteisesti anneta silloin, kuin virka-apupyynnön tekeminen ei perustu pyytävän viranomaisen lakisääteiseen toimivaltaan, tai kyseisen virka-avun antamisesta ei ole virka-apua antamaan pyydetyn viranomaisen toimintaan liittyen laissa määrätty. Lisäksi on huomioitava, että virka-apua voi nimensä mukaisesti pyytää vain viranomainen, eikä yksityishenkilöiden, yritysten tai yhteisöjen tukipyyntöjä voida lukea lakiperusteisiksi virka-apupyynnöiksi. (Tullin valvontapäällikkö 2022, Valvonta- ja hälytyssektorin komisario 2022, Lapsiperhetyön päällikkö 2022).

VIRKA-APUPROSESSI JATKUVUUDEN VARMISTAMISEN TYÖKALUNA

Virka-avusta on huomioitava, että virka-apupyynnöt ja virka-avun antamisen päätökset on dokumentoitava, ja kentällä tapahtuvan käytännön työn rinnalla virka-apuprosessia johdetaan virallisilla kirjallisilla pyynnöillä ja päätöksillä. Haastateltujen viranomaisten edustajien mukaan sekä kiireellinen että kiireetön virka-apu ja niihin liittyvien pyyntöjen käsittely toteutetaan usein hyvin samalla tavalla. Tästä poikkeuksen tekee Tulli, jonka edustajan mukaan kiireellisten ja ei-kiireellisten pyyntöjen käsittelyprosessi on erilainen, joskin niissäkin päätöksenteko tehdään yhtä lailla keskitetysti. Usein virka-apu valmistellaan kahden viranomaisen edustajan kanssa käytävillä suullisilla alustavilla keskusteluilla, sekä suullisilla virka-apupyynnöillä ja päätöksillä, jotka on myöhemmin vahvistettava kirjallisesti. Virka-avun valmistelut saadaan tarvittaessa kuitenkin käyntiin jo ennen virallisia kirjallisia päätöksiä. (Ensihoidon kenttäjohtaja 2022, Tilanne- ja johtokeskuksen Palopäällikkö 2022, Pelastustoiminnan palveluyksikön Palopäällikkö 2022, Lapsiperhetyön päällikkö 2022, Tullin Valvontapäällikkö 2022, Luukkola 2021).

> ***Yhteistoiminnan ja virka-avun tehokkaan toteutumisen näkökulmasta on keskeistä, että eri viranomaisten edustajat tuntevat toistensa suorituskyvyt ja kyvyn tukea tehtävässä.***

Haastatteluista ilmeni, että yhteistoiminnan ja virka-avun tehokkaan toteutumisen näkökulmasta on keskeistä, että eri viranomaisten edustajat tuntevat toistensa suorituskyvyt ja kyvyn tukea tehtävässä. Lisäksi henkilökohtainen tunteminen eri viranomaisorganisaatioiden edustajien kesken voi madaltaa kynnystä ensimmäisen yhteydenoton tekemiseen kumppaniorganisaatioon. Tätä voidaan jopa pitää kansallisen viranomaisyhteistyön yhtenä erityisenä vahvuutena (Ensihoidon kenttäjohtaja 2022, Tilanne- ja johtokeskuksen Palopäällikkö 2022, Pelastustoiminnan palveluyksikön Palopäällikkö 2022, Lapsiperhetyön päällikkö 2022, Tullin Valvontapäällikkö 2022, Luukkola 2021).

Virka-avusta ja sen toimeenpanoprosessista on kuitenkin huomioitava, että pääsääntöisesti selkeistä toimintatapamalleista huolimatta virka-apua ja sen johtamista on edelleen kehitettävä. Haastateltujen viranomaisten edustajien mukaan ajoittain ero virka-avun ja viranomaiselle lain mukaan kuuluvan hälytystehtävän ero on epäselvä. Ainakin haastatellun ensihoidon kenttäjohtajan mukaan prosessi vaatisi selkeytystä ja lain selkeyttämistä erityisesti terveydenhuollon toimintamahdollisuuksien osalta (Ensihoidon kenttäjohtaja 2022).

Lisäksi eri viranomaisorganisaatiot saavat turhia tai perusteettomia virka-apupyyntöjä, joita ei voida laillisten perusteiden puuttuessa toteuttaa. Osa viranomaisten edustajista myös piti virka-apuprosessia työläänä, koska virka-apumenettely vaatii kirjallisen pyynnön, kirjallisen päätöksen tiedoksiantoineen sekä erityistapauksissa annetusta tuesta laskuttamisen. Toisaalta virka-apuprosessia voidaan pitää myös eräänlaisena laadunvarmistusprosessina, jossa varmistutaan siitä, että virka-apupyyntö käsitellään vastaanottavassa viranomaisessa asianmukaisesti, ja toiminta perustuu viranomaisen toimintaa ohjaaviin lakeihin. Virka-apuprosessin keventämiselle on kuitenkin todettu olevan tilausta. (Valvonta- ja hälytysyksikön komisario 2022, Luukkola 2021).

POHDINTA

Virka-apu osaltaan mahdollistaa viranomaisten toiminnan jatkuvuuden turvaamisen tai lainkäytön tilanteessa, jossa päävastuuviranomaisen omat resurssit, suorituskyvyt tai toimivaltuudet eivät mahdollista tehtävän loppuun suorittamista omin avuin. Viranomaisyhteistyö ja virka-apu toimivat siten viranomaisten operatiivisen toiminnan jatkuvuuden varmistamisen työkaluina. Viranomaisten välistä yhteistoimintaa on mahdollista toteuttaa lakisääteisesti ilman virka-apumenettelyäkin, mistä hyvinä esimerkkeinä ovat esitelty Pelastuslain 46§ ja Laki poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta.

Vaikka viranomaisyhteistyötä ja virka-apumenettelyä voidaankin jossain määrin pitää kansallisina viranomaistoiminnan vahvuusalueina, on niissäkin edelleen kehitettävää. Artikkelia varten tehdyissä haastatteluissa esiin tulleiden mainintojen kautta on havaittavissa, että virka-apumenettely ei ole aina sitä soveltavan virkamiehen kannalta yksiselitteinen, selkeä tai riittävän ketterä. Yhteinen koulutus, harjoittelu ja henkilökohtainen tunteminen edesauttavat viranomaisten välistä yhteistoimintaa ja virka-avun toimeenpanoa. Viranomaisten toiminnan on kuitenkin perustuttava kaikissa tilanteissa hyvään hallintotapaan ja lakiin, joten näiden perusteiden on oltava kunnossa myös viranomaisyhteistoiminnan ja virka-avun osalta. Virka-avusta säädetään useassa laissa, eikä varsinaista erillistä virka-apua kokonaisuutena määräävää lakia ole. Tämän osalta tilannetta voisi selkeyttää kokoava erillislaki virka-avusta viranomaisten välillä.

Vaikka niin sanotussa viranomaisten arjessa useat vaativatkin tilanteet saadaan nykyisellään käytössä olevin yhteistoiminnan ja virka-avun menetelmin ratkaistua, ei viranomaisten välistä yhteistoimintaa ole juuri koeteltu viime vuosikymmeninä yhteiskunnallisilla poikkeusoloilla, pois lukien koronapandemian aikana julistetut poikkeusolot. Valmiuslaki kuitenkin edellyttää viranomaisia valmiussuunnitelmin ja muilla toimenpiteillä varmistamaan tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Artikkelin julkaisuhetkellä käsillä oleva eurooppalaisen turvallisuuden järkkyminen Ukrainan sodan johdosta herätteleekin tarkastelemaan, miten viranomaisten operatiivisen toiminnan jatkuvuus saadaan yhteistoiminnalla ja virka-apumenettelyllä varmistettua myös poikkeusoloissa.

Lähteet

Hallintolaki 434/2003. Viitattu 9.4.2022. *https://www.finlex.fi/fi/laki/ajantasa/2003/20030434*

Klemm, K. 2022. Huoltovarmuus – Varautumisella selviytymiskykyä. Helsinki: Tietosanoma.

Laki poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta 687/2009. Viitattu 9.4.2022. *https://finlex.fi/fi/laki/ajantasa/2009/20090687*

Laki Puolustusvoimien virka-avusta poliisille 781/1980. Viitattu 10.4.2022. *https://www.finlex.fi/fi/laki/ajantasa/1980/19800781*

Luukkola, O. 2021. Tukea tilanteessa kuin tilanteessa. Ruotuväki-lehti. Viitattu 10.4.2022. *https://ruotuvaki.fi/-/tukea-tilanteessa-kuin-tilanteessa*

Pelastuslaki 379/2011. Viitattu 9.4.2022. *https://www.finlex.fi/fi/laki/ajantasa/2011/20110379*

Puolustusvoimat 2022. Verkkosivut. Viitattu 10.4.2022. *https://puolustusvoimat.fi/osa-yhteiskuntaa/viranomaisyhteistyo*

Sisäministeriö 2019. Kansallinen riskiarvio 2018. Viitattu 9.4.2022. *http://urn.fi/URN:ISBN:978-952-324-245-6*

Valmiuslaki 1552/2011. Viitattu 9.4.2022. *https://www.finlex.fi/fi/laki/ajantasa/2011/20111552*

Valtioneuvosto 2017. Yhteiskunnan turvallisuusstrategia. Viitattu 9.4.2022. *https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf*

Valtonen, V. 2010. Turvallisuustoimijoiden yhteistyö operatiivis-taktisesta näkökulmasta. Maanpuolustuskorkeakoulu. Taktiikan laitos Julkaisusarja 1: No 3/2010. *https://urn.fi/URN:NBN:fi-fe201201241166*

Julkaisemattomat lähteet

L**apsiperhetyön päällikön sähköpostihaastattelu** 25.3.2022.

Pelastuslaitoksen tilanne- ja johtokeskuksen palopäällikön sähköpostihaastattelu 22.03.2022.

Pelastuslaitoksen pelastustoiminnan palveluyksikön palopäällikön haastattelu 11.3.2022.

Poliisin valvonta- ja hälytysyksikön komisarion sähköpostihaastattelu 22.03.2022.

Sairaanhoitopiirin kenttäjohtajan sähköpostihaastattelu 25.03.2022.

Tullin valvontapäällikön sähköpostihaastattelu 01.04.2022.

6 Turvallisuusteknologiat kyberympäristön luottamuksen työkaluina

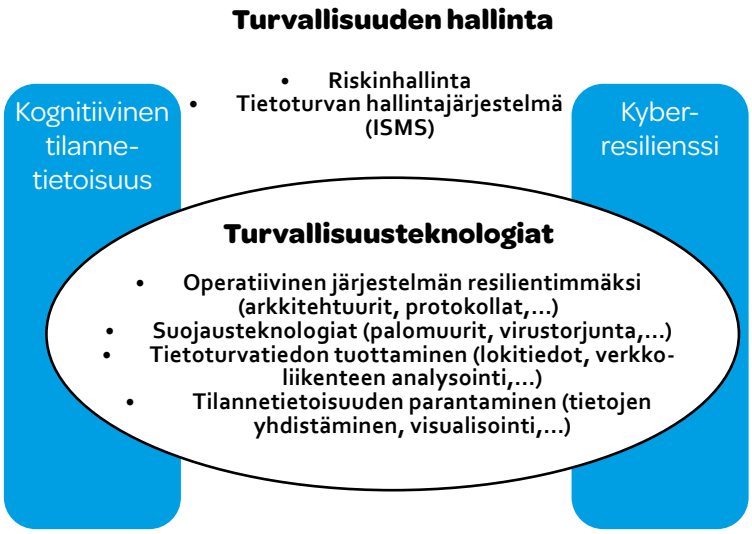
Jyri Rajamäki

KYBERTURVALLISUUSTUTKIMUS ON NUORI tutkimusalue, eikä se vielä ole saavuttanut yksimielistä tieteellistä määritelmää. Yleisen yhteisymmärryksen mukaisesti se tutkii kyber(toiminta)ympäristön (cyber space) turvaamista vahingoilta ja uhilta (Edgar & Manz, 2017). Turvallisuuskomitean (2018) määritelmän mukaan kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Myös kyberympäristölle on monia määritelmiä ja tässä artikkelissa se ymmärretään kokonaisuutena, joka sisältää tiedon, teknologian ja sosiaalisen näkökulman. Edgarin ja Manzin (2017) mukaan kyberturvallisuus tutkimusalana yhdistää informaatio-, insinööri- ja sosiaalitieteet. Lehdon ym. (2019) mukaan terveydenhuolto tietojärjestelmineen on hyvä esimerkki kyberympäristöstä.

Tämän teoreettisen artikkelin tarkoituksena on ymmärtää, miten luottamusta voidaan systemaattisesti rakentaa kybertoimintaympäristöön. Lisäksi artikkeli esittää uuden turvallisuusteknologioiden jaottelun, joka auttaa tiedostamaan minkälaisia turvallisuusteknologioita tämän luottamuksen rakentaminen vaatii.

KYBERYMPÄRISTÖN LUOTTAMUKSEN RAKENTAMISEN OSA-ALUEET

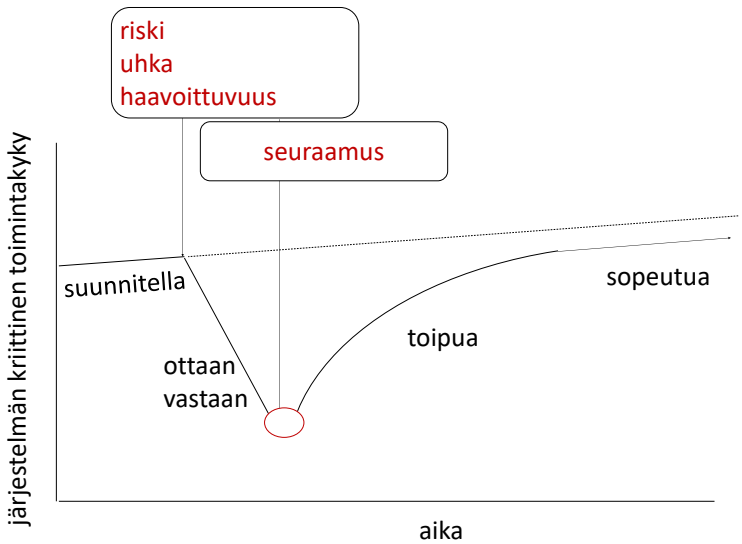
Digistaalisuuteen ja yhteiskehittämiseen erikoistuneen yrityksen, DIMECCin mallia mukaillen kyberympäristön luottamuksen rakentaminen koostuu kuvíon 1 mukaisesti neljästä osa-alueesta (DIMECC 2017). Ensimmäinen osa-alue ja koko luottamuksen rakentamisen päämäärä on *kyberresiliessi* eli operatiivisten järjestelmien resilienssi kyberympäristössä. Toinen osa-alue turvallisuuden hallinta ohjaa luottamuksen rakentamisen prosessia. Kolmas osa-alue ja kyberresilienssin ehdoton edellytys on *kognitiivinen tilannetietoisuus*. Neljännen osa-alueen muodostavat luottamuksen rakentamisen työkalut eli *turvallisuusteknologiat.*



Kuvio 1. *Kyberturvallisuuden ja -resilienssin teemat (muokattu lähteestä DIMECC 2017).*

KYBERRESILIENSSI

Ligon ym. (2021) mukaan kyberresilienssin käsite on kuvion 2 mukaisesti samanlainen kuin muiden tieteenalojen yleinen resilienssin määritelmä. Se sisältää neljä kyvykkyyttä: suunnitella ja valmistautua tunnettuihin tai tuntemattomiin uhkiin, ottaa uhka vastaan, toipua uhkasta ja lopuksi sopeutua uuteen normaaliin (National Academy of Sciences 2012).



Kuvio 2*. Resilienssisyklin kyvykkyydet*

Linkov ym. (2013) yhdistävät nämä kyvykkyydet kyberjärjestelmän mittareihin taulukon 1 mukaisesti neljällä tasolla: (1) fyysiset resurssit ja kyvykkyydet sekä näiden suunnittelu, (2) tieto ja tiedon kehittäminen fyysiseltä tasolta, (3) tasojen 1 ja 2 kognitiivinen hyödyntäminen päätösten tekemiseksi ja (4) sosiaalinen rakenne ja kommunikaatio kognitiivisten päätösten tekemiseen. Järjestelmän kyberresilienssiä voidaan arvostaa vain, kun riittävät resilienssitoimenpiteet määritellään ja toteutetaan (Ligo ym. 2021). Resilienssin rakentamisen prosessi on julkisten ja yksityisten sidosryhmien yhteinen toiminta, jolla vastataan infrastruktuurin häiriöihin (Heinimann & Hatfield 2017).

Taulukko 1. *Kyberresilienssimatriisi (Ligon ym. 2021)*

KYBER-JÄRJESTELMÄN TASO	RESILIENSSISYKLIN VAIHE			
	SUUNNITTELU	VASTAANOTTO	TOIPUMINEN	SOPEUTUMINEN
FYYSINEN	Laitteiden tila ja valmiudet, verkoston rakenne	Tapahtuman toteaminen, järjestelmän suorituskyky toimintojen ylläpitämiseksi	Järjestelmämuutokset toiminnallisuuden palauttamiseksi	Uuden normaalin vaatimat muutokset, resilienssin parantaminen
INFORMAATIO	Tiedon muokkaaminen, valmistelu, esittäminen ja varastointi	Reaaliaikainen toiminnallisuuden arviointi, kasautumien menetysten ennakointi ja tapahtuman päättäminen	Tiedon hyödyntäminen toipumisen edistämiseksi ja palautumisskenaarioiden ennakoimiseksi	Tiedon varastoinnin ja hyödyntämisen protokollien luominen ja parantaminen
KOGNITIIVINEN	Järjestelmän suunnittelu ja toimintaa koskevat päätökset uhkaa silmälläpitäen	Ehdolliset protokollat ja ennakoiva tapahtuman hallinta	Palautumista koskeva päätöksenteko ja viestintä	Uusien järjestelmämäärittelyjen suunnittelu, tavoitteet ja päätöskriteerit
SOSIAALINEN	Henkilöstä, sosiaalinen verkosto, ja pääoma, kulttuuriset normit, harjoitus, koulutus	Neuvokas ja saatavilla oleva henkilöstö sekä sosiaaliset instituutiot tapahtumaan reagoimiseksi	Ryhmätyö ja tiedon jakaminen järjestelmän palautumisen vahvistamiseks	Muutokset instituutioissa, politiikoissa, koulutusohjelmissa ja toimintakulttuurissa

TURVALLISUUDEN HALLINTA

Turvallisuusjohtaminen keskittyy järjestelmän jatkuvaan hallintaan ja toimintaan luomalla dokumentoidut systemaattiset menettelyt ja prosessit. Tietoturvallisuusmenettelyillä saavutetaan organisaation tietoresurssien luottamuksellisuus, eheys ja saatavuus. Painopistealueita ovat turvallisuuspolitiikan kehittäminen ja toteuttaminen, riskienhallinta, tietoturvainvestoinnit, kannustimet ja kompromissit.

Jos kyberturvallisuusriskeihin ei varauduta, organisaatiot kohtaavat ajan mittaan vakavia katastrofeja. Organisaation näkökulmasta kyberturvallisuuden hallinta lähtee liikkeelle riskienhallintamenettelystä. Riskienhallinnan tutkimus keskittyy kyberturvallisuuden tilan mittaamiseen ja kvantifiointiin, mukaan lukien kyberturvallisuuden arvon kvantifiointi toiminnalle, kuinka suurelle uhalle toiminta on alttiina ja pisteytetään, kuinka lievennykset ja turvakontrollit vaikuttavat kokonaistoimintariskiin (Edgar & Manz 2017).

Nykyisin organisaatiot ovat yhä riippuvaisempia ennakoimattomista ja tuntemattomista kyberturvallisuusriskeistä, joita perinteisellä riskinarvioinnilla ei voi hallita. Kaikkialla läsnä oleva tietojenkäsittely tarkoittaa, että organisaatiot eivät tiedä, milloin ne käyttävät luotettavia laitteita tai palveluita, ja niissä on ketjureaktioita ennakoimattomista riskeistä.

Tietoturvan hallintajärjestelmä *(information security management system, ISMS)* tarjoaa ohjaimia organisaation tärkeimmän omaisuuden, tiedon, suojaamiseksi. Monet organisaatiot soveltavat auditointeja ja sertifiointeja ISMS:ään vakuuttaakseen sidosryhmänsä siitä, että organisaation turvallisuus on asianmukaisesti hallittua ja että se täyttää säädösten turvallisuusvaatimukset. Tietoturva-auditointi on organisaation tietoturvatason auditointi. Turvatietoiset asiakkaat voivat vaatia ISMS-sertifioinnin ennen liikesuhteen solmimista.

Nykyisin yleisimmät tietotekniikan turvallisuusstandardit ovat ISO/IEC 27001:2013 Tietoturvan hallintajärjestelmävaatimukset, ISO/IEC 27002:2013 Tietoturvaohjauksen käytännesäännöt ja ISO/IEC 27005:2018 Tietoturvariskien hallinta. Valitettavasti IT-tietoturvastandardit eivät ole täydellisiä ja niissä on mahdollisia ongelmia. Yleensä ohjeet laaditaan käyttämällä yleisiä tai universaaleja malleja, jotka eivät välttämättä koske kaikkia organisaatioita. Yleisiin, perinteisiin käytäntöihin perustuvissa ohjeissa on otettu huomioon organisaatioiden erot ja organisaatiokohtaiset turvallisuusvaatimukset.

KOGNITIIVINEN TILANNETIETOISUUS

Kognitiivinen tilannetietoisuus on kyberturvallisuuden ja -resilienssin pääedellytys, jota ilman on mahdotonta systemaattisesti estää, tunnistaa ja suojata järjestelmää kybertapahtumilta ja kyberhyökkäyksen sattuessa toipua hyökkäyksestä (Rajamäki 2021). Se tarkoittaa, että olet tietoinen siitä, mitä järjestelmäsi ympärillä tapahtuu, jotta ymmärrät, kuinka tiedot, tapahtumat ja toimintasi vaikuttavat päämääriin ja tavoitteisiin nyt ja pian. Se mahdollistaa myös tehokkaiden ja tehokkaiden vastatoimien valinnan ja suojaa siten järjestelmää erilaisilta uhilta ja hyökkäyksiltä (DIMECC 2017).

Tilannetietoisuutta kyberympäristössä el*i kybertilannetietoisuutta* tarvitaan pohjaksi vastatoimien (kont-

> ***Kognitiivinen tilannetietoisuus on kyberturvallisuuden ja -resilienssin pääedellytys, jota ilman on mahdotonta systemaattisesti estää, tunnistaa ja suojata järjestelmää kybertapahtumilta ja kyberhyökkäyksen sattuessa toipua hyökkäyksestä.***

rollien) kehittämiselle ja hyödyntämiselle. Kybertilannetietoisuuden tärkeimmät mahdollistajat ovat havainnot, analyysi, visualisointi, valtion kyberpolitiikka sekä kansallinen ja kansainvälinen yhteistyö. Asiaan liittyvää päätöksentekoa varten tarvitaan kyberympäristön eri lähteistä kerättyä relevanttia tietoa, esim. verkot, riskitrendit ja toimintaparametrit.

Digitaalinen kaksonen tarkoittaa digitaalista kopiota fyysisistä prosesseista, jotka sisältävät ihmisiä, järjestelmiä ja laitteita (Grieves & Vickers 2017). Digitaalinen kaksonen rakennetaan esimerkiksi pilvipalveluun ja sen on tarkoitus toimia reaaliaikaisesti. Eckhart, Ekelhart ja Weippl (2019) esittelevät digitaaliseen kaksoseen perustuvan kyberympäristössä toimivan järjestelmän tilannetietoisuuskehyksen, joka tarjoaa syvällisen, kokonaisvaltaisen ja ajankohtaisen näkemyksen kybertilanteesta.

TURVALLISUUSTEKNOLOGIAT

Turvallisuusteknologioita hyödynnetään kyberympäristön luottamuksen rakentamisessa eri tarkoituksiin. Ensinnäkin niiden avulla operatiivinen järjestelmä rakennetaan mahdollisimman turvalliseksi. Toiseksi niillä luodaan tietoturvatietoja operatiivisesta järjestelmästä ja sen suojauksesta sekä siirretään niitä tilannetietoisuuden muodostamiseksi. Kolmanneksi niitä käytetään operatiivisen järjestelmän suojaamiseen. Neljänneksi turvallisuusteknologioilla koostetaan tilannetietoisuutta sekä visualisoidaan ajantasainen tilannekuva. Useat turvallisuusteknologiat toteuttavat useampaa kuin yhtä edellä luetelluista tarkoituksista.

Operatiivisen järjestelmän turvallisuuden parantamiseen tähtäävät turvallisuusteknologiat sisältävät kaikki ne kyberturvallisuuden tekniset keinot, joita hyödynnetään turvallisten järjestelmien kehittämisessä ja käyttöönotossa. Näitä ovat tietoturvalliset järjestelmäarkkitehtuurit, protokollat ja toteutukset, sekä erilaiset kehittämistyökalut ja alustat.

Tekniikat, jotka luovat ja siirtävät tietoturvatietoja operatiivisesta järjestelmästä kognitiiviseen tilannetietojärjestelmään sisältävät antureita, jotka keräävät ensimmäisen tason dataa (Rajamäki 2021). Monet isäntä- ja verkkopohjaiset työkalut luovat tapahtumalokeja, joita käytetään tilannetietoisuuden luontiin. Myös verkkoliikenteen analysoijat ja tunkeutumisen havainnointijärjestelmät keräävät tietoturvatietoa.

Kolmannen päätarkoitukseen mukaiset turvallisuusteknologiat mahdollistavat infrastruktuurien, alustojen, laitteiden, palveluiden ja tietojen teknisen suojauksen. Tekninen suojaus alkaa turvallisella käyttäjän tunnistamisella ja valtuutuksilla, jotka ovat välttämättömiä ominaisuuksia useimmissa turvallisissa infrastruktuureissa, alustoissa, laitteissa ja palveluissa. Onneksi niiden toteuttamiseen on olemassa tunnettuja tekniikoita. Tyypillisesti prosessit ja tieto-objektit liitetään omistajaan, jota edustaa tietokonejärjestelmässä käyttäjätili, joka asettaa käyttöoikeudet muille. Tunnettuja tietoturvateknologiastandardeja ovat ISO/IEC 27033:2015 Verkkoturvallisuus, ISO/IEC 27034:2015 Sovellusturvallisuus ja ISO/IEC 27036-1:2014 Toimittajasuhteiden tietoturva.

Teknologioita, jotka sekä suojaavat että tuottavat tietoturvatietoa ovat muun muassa allekirjoituspohjaiset työkalut, kuten virustorjunta- ja tunkeutumisen havaitsemisjärjestelmät. Nämä teknologiat ovat tiivistäneet aiemman tiedon havaituista hyökkäyksistä allekirjoituksiksi, jotka havaitsevat ja hälyttävät, kun hyökkäyksiä havaitaan operatiivisissa järjestelmissä. Kehittyneemmät järjestelmät, kuten tietoturvatiedot ja tapahtumanhallintajärjestelmät *(security information and event manager, SIEM)*, tarjoavat infrastruktuurin, joka kokoaa yhteen tietojoukot useista antureista korrelaatioiden suorittamista varten. Haavoittuvuusanalyysi sen määrittämiseksi, kuinka monta korjaamatonta haavoittuvuutta järjestelmästä löytyy, on myös tason kaksi teknologiaa.

Kuvio 3 esittää kognitiivisen tilannetietoisuusjärjestelmän teknisen periaatteen. Se perusta on datafuusiomoottori, joka yhdistää eri lähteistä saamaansa tietoa. Lisäksi se sisältää tietorajapinnat sekä käyttöliittymän, joka tarjoaa visualisointikerroksen ja jonka avulla operaattori voi ohjaa antureita ja datafuusioalgoritmeja sekä tarvittaessa syöttää tietoja järjestelmään. (Kokkonen 2016.)

Kuva 3: *Kognitiivisen tilannetietoisuuden arkkitehtuuri (muokattu lähteestä Kokkonen 2016).*

YHTEENVETO JA JOHTOPÄÄTÖKSET

Investoimalla teknisiin järjestelmiin, jotka lisäävät luottamuksellisuutta *(confidence)* ja luottamusta *(trust),* voidaan merkittävästi vähentää kustannuksia ja nopeuttaa vuorovaikutusta. Kyberturvallisuuden yleisenä tavoitteena on, että kaikki toimintajärjestelmät ja infrastruktuurit ovat resilienttejä. Tästä näkökulmasta turvallisuusteknologiat ovat keskeisiä mahdollistajia luottamuksen kehittymiselle ja ylläpitämiselle digitaalisessa maailmassa. Taulukko 2 sisältää esimerkkejä turvallisuusteknologioista jaoteltuna niiden käyttötarkoituksen mukaan.

Taulukko 2. *Turvallisuusteknologioiden jaottelu käyttötarkoituksen mukaan*

TILANNE-TIETOISUUDEN PARANTAMINEN	SUOJAUS-TEKNOLOGIAT	TIETOTURVA-TIEDON TUOTTAMINEN	OPERATIIVISEN JÄRJESTELMÄN TURVALLISUUDEN PARANTAMINEN
Tietoturvatiedon yhdistäminen ja visualisointi, Tietoturvatiedon jakaminen, Digitaalinen kaksonen	Käyttäjän tunnistus ja valtuutus, Palomuurit, Virustorjuntaohjelmat, Tunkeilijan torjuntajärjestelmä (IPS), SIEM-järjestelmät (Security Information and Event Management)	Lokitiedot suojausteknologioista ja operatiivisen järjestelmän tapahtumista, Verkkoliikenteen analysoijat, Tunkeilijan havaitsemisjärjestelmät (IDS)	Järjestelmäarkkitehtuurit, Protokollat, Toteutukset, Kehittämistyökalut- ja alustat

Turvateknologioita tarvitaan myös silloin, kun jotain on tapahtunut. Esimerkiksi tietoturvaloukkausten tutkinta, ns. IT-forensiikka, pyrkii löytämään hyökkäyksen/virheen lähteet ja tarjoamaan tietoa ongelman oikeudellisista ja muista seurauksista. IT-forensiikka helpottaa myös tapahtuman syiden analysointia, mikä puolestaan mahdollistaa vastaavien hyökkäysten oppimisen ja välttämisen tulevaisuudessa.

Lähteet

DIMECC. 2017. The Finnish Cyber Trust Program 2015–2017. Helsinki: DIMECC. *https://www.dimecc.com/wp-content/uploads/2019/06/DIMECC_PUBLICATIONSSEREISNO20_CyberTrust.pdf*

Eckhart, M., Ekelhart, A. & Weippl, E. 2019. Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins. 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 1222-1225.

Edgar, T. & Manz, D. 2017. Research methods for cyber security. Cambridge: Syngress.

Grieves, M. & Vickers, J. 2017. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Teoksessa Kahlen, F-J. Flumerfelt, S. & Alves, A. (toim.). Transdisciplinary Perspectives on Complex Systems. Berlin: Springer, 85-113.

Heinimann, H. & Hatfield, K. 2017. Infrastructure Resilience Assessment, Management and Governance – State and Perspectives. Teoksessa Linkov, I. & Palma-Oliveira, J. M. (toim.). Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security. Cham: Springer, 147-187.

Kokkonen, T. 2016. Anomaly-Based Online Intrusion Detection System as a Senor for Cyber Security Situational Awareness System. Jyväskylä Studies in Computing 251. Jyväskylä: Jyväskylän yliopisto. *http://urn.fi/URN:ISBN:978-951-39-6832-8*

Lehto, M., Pöyhönen, J. & Lehto, M. 2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa, Loppuraportti, Vol. 2. Jyväskylä: Jyväskylän yliopiston IT-tiedekunta. *http://urn.fi/URN:ISBN:978-951-39-7711-5*

Ligo, A., Kott, A. & Linkov, I. 2021. How to Measure Cyber Resilience of an Autonomous Agent: Approaches and Challenges. 1st International Conference on Autonomous Intelligent Cyber-defence Agents. Pariisi, Ranska.

Linkov, I., Eisenberg, D. A., Plourde, K, Seager, T. P., Allen, J. & Kott, A. 2013. Resilience metrics for cyber systems. Environ Syst Decis. 47, 10108–10110.

National Academy of Sciences. 2012. Disaster resilience: a national imperative. *https://doi.org/10.17226/13457*

Rajamäki, J. 2021. Resilience Management Concept for Railways and Metro Cyber-Physical Systems. Teoksessa Eze, T. (toim.). Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS. Reading: Academic Conferences International Limited, 337-345.

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry. *https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/*

7 Kyberuhkiin varautuminen riskienhallinnan, jatkuvuuden ja kyberresilienssin keinoin

Jari Marttinen, Elina Partanen, Markus Saario & Mikko Ylivakeri

JOHDANTO

KYBERUHKAT JA -RESILIENSSI ovat nousseet trendiaiheiksi vuoden 2022 aikana. Molemmat vaikuttavat organisaatioiden jatkuvuudenhallintaan, jossa riskienhallinnan ohella uhkakeskeinen kyberturvallisuudenhallinta on tärkeässä osassa.

Jo vuonna 2017 Euroopan komissio on pohdinta-asiakirjassaan analysoinut Euroopan uhkakuvia. Digitaalisuus, big data, pilviteknologia sekä tekoäly tulevat muovaamaan yhteiskuntien rakenteita ja niiden luonnetta aina turvallisuus ja puolustus mukaanluettuna. Uuden teknologian käyttö mahdollistaa valtioiden rajat ylittävien hybridi- ja kyberuhkien nopean kasvun. Tämä on huomattu myös Suomessa mm. vuoden 2017 puolustusselonteossa, missä kyberympäristön merkityksen on todettu kasvavan. (Lehto 2021, 2-3; Euroopan komissio 2017; Valtioneuvoston puolustusselonteko 2017, 9.)

Venäjän aloitettua hyökkäyssodan Ukrainassa, on hybridi- ja kybervaikuttamisen uhka kasvanut myös Suomessa huomattavasti. Vaikka Suomeen ei ole kohdistunut mitään suurempaa uhkaa kybermaailmassa, eivätkä sodan kybervaikutukset ole näkyneet Suomessa huomattavissa määrin (Kybersää helmikuu 2022), on Suomessa nostettu varautumista mahdollisiin kyberuhkiin valtion ylimmässä johdossa ja monella toimialalla (Valtiovarainministeriö 2022; Finanssivalvonta 2022).

Tässä artikkelissa tarkastellaan, kuinka kyberuhkiin voidaan varautua riskienhallinnan, jatkuvuuden ja kyberresilienssin keinoin. Nämä ovat niitä keskeisiä keinoja, minkä avulla pystytään suojamaan yrityksiä ja organisaatioita yllätyksellisiltä ja äkillisiltä uhilta (Ruoslahti 2021).

Artikkelin teoreettisena perusteena käytetään painettua lähdekirjallisuutta, artikkelijulkaisuja, sähköisiä lähteitä ja asiantuntijahaastatteluja. Asiantuntijahaastatteluissa käsiteltiin toiminnan jatkuvuutta Cyber Resilience Managerin sekä ICT-alan jatkuvuuden hallinnan asiantuntijan näkökulmasta. Artikkeli perustuu lähdemateriaalien tutkimiseen ja analysointiin aiemmin esitetystä näkökulmasta.

RISKIENHALLINTA

Modernin riskienhallinnan historian katsotaan alkaneen toisen maailmansodan jälkeen 1950-luvulla. Riskienhallinnan synty kytkeytyy vahvasti vakuutuksiin, jotka ovat olleet ensimmäisiä konkreettisia keinoja riskienhallinnaksi. Kuitenkin vasta 1970- ja 1980-luvuilla riskienhallinnasta alkoi tulla suurempi osa yritysten liiketoimintaa. (Dionne 2013, 2.)

Mutta mitä sanalla riski tarkoitetaan? Eri instituutiot ja henkilöt määrittelevät riskin hieman eri tavoin. Tähän vaikuttaa muun muassa se, mihin kontekstiin määritelmä on tehty. Yksi tapa määritellä riski on, että sillä tarkoitetaan suunnittelematonta tapahtumaa, jolla on yllättäviä vaikutuksia (Hopkin 2018, 16). Toisena esimerkkinä on Suomen Huoltovarmuuskeskuksen määritelmät, joiden mukaan riski on todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai, että se on uhkaan liittyvän vahingon rahallinen odotusarvo (Huoltovarmuuskeskus 2022).

Miten riskejä vastaan voisi varautua tai miten niitä voisi hallita juuri kyberturvallisuuden kontekstissa? Ja tehdä tämä erityisesti aikana, jolloin pelkän kyberrikollisuuden kustannusten on arvioitu nousevan vuosittain 15 prosentilla, saavuttaen vuonna 2025 globaalisti 10.5 biljoonan USD kustannukset. Summaa hahmottaakseen voi ajatella, että valtion talouden suuruudessa mitattuna se olisi kolmanneksi suurin talous Yhdysvaltojen ja Kiinan jälkeen. Edelliseen pohjaten voidaan ainakin perustellusti todeta, ettei kyberturvallisuuden riskienhallinnalta tule sulkea silmiään. (Morgan 2020.)

Kyberturvallisuuden riskienhallintaan liittyy yleensä vähintään kaksi tekijää, järjestelmät/laitteet ja ihmiset. Tällä tarkoitetaan, että osa riskeistä syntyy toimintaympäristössä toimivista ihmisistä; heidän osaamisestaan ja tehdyistä inhimillisistä virheistä. Mikäli tällaisia henkilöstön aiheuttamia riskitekijöitä havaitaan, yksi tehokkaimmista keinoista on lisätä aiheeseen liittyvää koulutusta. Kyberturvallisuuden osin teknisen luonteen vuoksi on mahdollista, että riskejä aiheutuu suoraan tai välillisesti organisaation käyttämistä teknisistä ratkaisuista. Näin voi käydä, mikäli käytettyjä teknisiä ratkaisuja ei tunneta kunnolla tai niitä ei valita oikein, huomioiden toimintaympäristön vaatimukset. Tämän osalta helpoimmat askeleet parempaan riskienhallintaan on, että organisaatio huolehtii käyttämiensä järjestelmien ja laitteiden 1) tarkoituksenmukaisuudesta, 2) ylläpidosta ja 3) suojaamisesta. Osa organisaatioista hakee näihin toimiin apua ulkoistamisesta, jolloin esimerkiksi päivityksistä huolehtii ulkopuolinen tietoturvallisuusyritys. (Cyber Resilience Manager 2022; Isotalo 2022.)

Edellä mainitut tai niitä tarkemmat toimet eivät kuitenkaan toimi, mikäli kyberturvallisuudella ei ole todellista ja pysyvää asemaa organisaation riskienhallintakulttuurissa. Kyberturvallisuuden riskejä on arvioita ja hallittava samalla tavalla, kuin muitakin organisaation kohtaamia riskejä (Kyberturvallisuuskeskus 2021). Monissa organisaatioissa tämä saattaa vaatia ajattelutavan muutosta. Päivittämätön sähköpostijärjestelmä on riski samalla tavalla kuin lukitsematon kassakaapin ovi.

JATKUVUUDENHALLINTA

Jatkuvuudenhallinta kyberriskien kontekstissa

Yritysten tulee huolehtia liiketoiminnan jatkuvuudesta poikkeamatilanteissa, ja poikkeamatilanteisiin tulee varautua suunnitelmallisesti jo ennalta. Jos yritys ei kykene reagoimaan poikkeamiin ja palauttamaan toimintaansa poikkeamaa edeltävälle tasolle, yrityksen koko olemassaolo voi vaarantua. Jatkuvuudenhallinta on siis riskienhallintaa, ja tietoturva- ja tietosuojariskien huomioiminen on keskeistä yritysten jatkuvuudenhallinnalle. (Jatkuvuudenhallinnan asiantuntija, 2022.)

Nykyään valtaosa yritysten turvallisuuspoikkeamista liittyy tietoturvaan, koska tietotekniikkaa ja uusia teknologioita omaksutaan käyttöön enenevässä määrin, etätöiden tekeminen lisääntyy, ja yritykset siirtyvät fyysisten hardware-palvelimien käytöstä halvempiin pilvipalveluratkaisuihin. Tietotekniikka aiheuttaa myös sen, että poikkeamatilanteissa esimerkiksi tietovuoto voi nopeasti laajeta ison yleisön saataville, tai vaikka itse poikkeama saataisiin hallittua, niin tieto tietoturvapoikkeamasta voi silti levitä nopeasti ja aiheuttaa mainehaittaa. (Jatkuvuudenhallinnan asiantuntija, 2022.) Vaikka iso osa turvallisuuspoikkeamista liittyykin tietotekniikkaan, yritysten työntekijät eli ihmiset ovat kuitenkin edelleen juurisyynä valtaosaan ongelmista tai ongelmien laajentumisesta (Swinfen Green & Dorey, 2016, luku 2).

> ***Jos yritys ei kykene reagoimaan poikkeamiin ja palauttamaan toimintaansa poikkeamaa edeltävälle tasolle, yrityksen koko olemassaolo voi vaarantua.***

Jatkuvuudenhallintajärjestelmän toteuttaminen

Yritysten jatkuvuudenhallinnalle keskeistä on jatkuvuudenhallintajärjestelmä, joka toimii tarvittaessa, mikäli poikkeamia sattuu. Yritysten tulee siis määritellä jatkuvuudenhallintajärjestelmänsä myös tietoturvapoikkeamien osalta niin, että se täyttää yrityksen tarpeet ja varmistaa, ettei resursseja hukata tarpeettomasti.

Olennaisia huomioitavia seikkoja jatkuvuudenhallintajärjestelmää luotaessa on ymmärtää mahdollisten tietoturvapoikkeamien vaikutukset ja niiden aiheuttamien toiminnankeskeytysten vakavuus, sekä luoda ja dokumentoida varautumis- ja palautumissuunnitelmat, jotka pohjautuvat realistisiin arvioihin poikkeamatilanteista. Suunnitelmien tulee pyrkiä palauttamaan riittävä toiminnallinen taso poikkeamien jälkeen, ja suunnitelmien laatijoiden tulisi olla itse lähellä sitä yrityksen toimintoa, jota suunnitelmat koskevat, ettei suunnittelu olisi irtonaista ja päälle liimattua. Myös riittävän resursoinnin varmistaminen poikkeamatilanteiden hoitamiseen ja palautumiseen on olennaista, samoin kuin suunnitelmien ja resurssoinnin toiminnan varmistaminen harjoittelemalla. (Rittinghouse & Ransome, 2011, luku 1.)

Haastavaksi jatkuvuudenhallinnan tekee se, että jatkuvuussuunnittelu ja pahimpaan varautuminen ei yleensä ole yritysten ydintoimintaa tai laskutettavaa liiketoimintaa, ja kuten yritysturvallisuus yleisestikin, jatkuvuussuunnittelu koetaan abstraktina ja ehkä jopa tarpeettomana, jos suunnitelmien päätavoitteena on, että niitä ei koskaan tarvitsisi käyttää (Jatkuvuudenhallinnan asiantuntija, 2022). Näinpä yksi tärkeimmistä asioista, joka jatkuvuudenhallintajärjestelmää luodessa tulisi varmistaa on ylimmän johdon tuki toiminnalle. Turvallisuus- ja jatkuvuudenhallinta-asiat tulisi kirjata yritysten strategioihin ja politiikkoihin, ja tätä tulisi viestiä koko organisaation laajuisesti ylimmältä johdolta alas liiketoimintayksiköille, ja liiketoiminnasta jopa yrityksen asiakkaille, alihankkijoille ja toimitusketjuille asti. On myös huomionarvoista, että jatkuvuudenhallintajärjestelmän käyttöönotto ei ole mikään kertasuorite, vaan iteratiivinen prosessi, jota pitää jatkuvasti katselmoida ja kehittää. (Calder, 2020, luku 4.)

Jatkuvuudenhallintajärjestelmän testaaminen

Kyberhäiriöt ovat yleensä yllätyksellisiä ja vaikutuksiltaan potentiaalisesti mittavia, ja niiden torjunta on valitettavan usein reaktiivista. Ennaltaehkäisevinä toimenpiteinä erityisesti tietojärjestelmien osalta pidetään tietoturvatestausta, oli kyse sitten ohjelmointikoodiin liittyvästä testauksesta tai laajemmasta ns. hyökkäävästä Red Team -tyyppisestä simuloidusta hyökkäyksestä toimitiloihin ja järjestelmiin. Harjoittelu on tärkeää, jotta saadaan todennettua, että laaditut suunnitelmat oikeasti toimivat. Myös erilaiset yhdistellyt hyökkäävät ja puolustavat tunkeutumisharjoitukset eli ns. Purple Team -toiminta voivat auttaa yrityksiä tunnistamaan tietoturvariskejä, joita vastaan tulisi varautua, sekä myös varautumiskeinoja (Jatkuvuudenhallinnan asiantuntija 2022.)

Yritysturvallisuuden parissa työskentelevät yleensä tiedostavat realistisen harjoittelun tärkeyden, koska se on paras tapa testata yrityksen varautumista ja jatkuvuussuunnitelmia käytännössä. Hyvin johdetulla harjoitustoiminnalla saadaan haastettua henkilöstöä tietoturvapoikkeamatilanteissa, ja usein myös harjoittelevat yksiköt ryhmäytyvät paremmin kohdatessaan yhdessä haasteita. Vaikka yksittäisen harjoitteluskenaarion osalta toiminta ei täyttäisikään tavoitteita, organisaatio ja henkilöt oppivat aina jotain poikkeamienhallinnasta, ja palautekeskustelut tuottavat usein toteutuskelpoisia parannusehdotuksia jatkuvuudenhallintajärjestelmään.

Isojen ja laajamittaisten, organisaatiorajat ylittävien harjoitusten järjestäminen on aikaa vievää, ja harjoitukset sitovat henkilöstöä. Usein täytyy myös etukäteen suunnitella, että tarvittavat henkilöt ovat varmasti saatavilla harjoitukseen, mikä hieman heikentää harjoituksen realismia. Toisaalta samoja asioita voidaan harjoitella myös pienemmillä harjoitteilla, vähemmällä valmistelulla, ja vaikka lyhemmät harjoitukset eivät ehkä ole yhtä mukaansatempaavia, niin näistä saadut oppimiskokemukset ovat silti hyödyllisiä yrityksen jatkuvuudenhallinnalle. (Maclean-Bristol, 2020, luku: Why Conduct Exercises.)

KYBERRESILIENSSI

Kyberresilienssi on tämän hetken trendi kyberturvallisuuden varautumisessa, mutta mitä termi pitää sisällään?

Resilienssin käsite on ollut jo ennen liiketoiminta- ja kyberympäristöä käytössä lääketieteessä, jossa resilienssi on tarkoittanut yksilön psykologista sietokykyä ja esimerkiksi traumasta palautumisen kyvykkyyttä. Kyberturvallisuudessa resilienssi tarkoittaa samankaltaisia asioita, mutta organisaation tietojen ja järjestelmien luottamuksellisuuden, saatavuuden ja eheyden näkökulmasta. Ihmisen ollessa psykofyysinen kokonaisuus, on kyberresilienssi samaan tapaan moniulotteinen kokonaisuus. (Carias, Borges, Labaka, Arrizabalaga & Hernantes 2020, 174200- 174201; Herrmann, Stewart, Diaz-Granados, Berger, Jackson & Yuen 2011, 258.)

Kyberresilienssiin vaikuttavat organisaation toimintaympäristö, sen hallinnointi, organisaation turvallisuustietoisuus ja jatkuvuudenhallinnan kokonaisuus sekä organisaation kyberturvallisuuden strategiset valinnat. Operatiivisella tasolla kyberresilienssin rakennuspalikoita ovat esimerkiksi politiikat, sopimukset ja toimintamallit ulkoisten sidosryhmien kanssa. Kyberresilienssi tukee liiketoiminnan kokonaisresilienssiä, jossa mitataan organisaation kykyä muuntua ulkoisen ympäristön mukana ja kestää sen aiheuttamia paineita. (Carias ym. 2020, 174200- 174201; ServiceNow™ 2022.)

Kyberresilienssin elinkaari voidaan määritellä viidellä Carias ym. (2020) esittämällä iteraation osalla, jotka ovat ennakoi, havaitse, kestä ja minimoi, palaudu ja kehity. Esitetty iteraatioprosessi tukee kokonaisvaltaisesti liiketoiminnan jatkuvuutta ja toimintamallia, jossa häiriö tai poikkeama hallitaan ilman paniikkia, dokumentoitujen käytäntöjen mukaisesti. Liiketoiminnan resilienssin yksi tarkoitus on tarkkailla kilpailuympäristöä ja tehdä strategisia toimenpiteitä sen perusteella. (Carias ym. 2020, 174201- 174202; Cyber Resilience Manager 2022.)

Kyberresilienssiin voi soveltaa samanlaista mallia, jossa kilpailuympäristö on julkisuuteen tai verkostoon nousseet poikkeustilanteet. Tilannekuvan muodostaminen ja ylläpito on iteraatioprosessin ennakoinnin perusta. Havaitseminen toteutuu organisaation kyberympäristön tapahtumamonitoroinnilla ja havainnointityökaluilla. Monitoroinnissa ja havaitsemisessa on tärkeää, että reunaehdot sellaisille häiriöille, jotka vaarantavat kyberturvallisuuden, on määritelty. Eskalointikäytäntöjen tulee olla selvillä, jotta reagointikyvykkyys ja siirtyminen seuraavaan vaiheeseen voidaan turvata. (Carias ym. 2020, 174201- 174202; Cyber Resilience Manager 2022; Niemimaa, Järveläinen, Heikkilä & Heikkilä 2019, 208-216.)

Häiriötilanteen kestäminen ja negatiivisten vaikutusten minimointi prosessissa on osa jatkuvuuden- tai poikkeamienhallintaa. Prosessin vaihe sisältää myös oletuksen, että häiriöltä pyritään suojaamaan muita haavoittuvia kohteita. Palautuminen on yksinkertaistettuna vaihe, jossa palataan normaalitilaan. Palautumisharjoittelua tulisi tehdä ja sillä on suuri merkitys todellisen häiriötilanteen sujuvuuden kannalta. Iteraatioprosessin vaihe, kehity, on tärkeä organisaation oppimisen kannalta. Vaiheessa tarkastellaan häiriötilannetta jälkikäteen ja muodostetaan kuva siitä, miten tilanne voitaisiin estää jatkossa tai miten reagointikyvykkyyttä voitaisiin parantaa. Kyberresilienssin ei, kuten ei kyberturvallisuudenkaan, pidä pyrkiä täydellisyyteen liiketoiminnan kehittämisen kustannuksella. (Carias ym. 2020, 174201- 174202; Cyber Resilience Manager 2022; Niemimaa & ym. 2019, 208-216.)

Toteuttavatko kaikki organisaatiot kyberresilienssinhallintaa samanlaisilla painopistealueilla? Annarelli ym. (2020) tutkimuksessa löydettiin kyberturvallisuuden tyypillisistä hallintakeinoista kyberresilienssinhallintaan yhdistävinä tekijöinä vain datan varmuuskopiointi, tietoturvatestaus, haavoittuvuuksien hallinta, audit-lokitus ja koulutus. Muut kyberturvallisuuden hallintakeinot ohjautuivat toimialakohtaisesti osaksi kyberresilienssinhallintaa. Hajontaa hallintakeinoissa tulee myös organisaation koon kautta. Suurilla organisaatioilla on tyypillisesti paremmat mahdollisuudet allokoida henkilöstöä kyberturvallisuuden tehtäviin ja ostaa esimerkiksi ulkopuolista havainnointi- ja hälytyspalvelua ympäri vuorokauden. Mitä paremmin organisaatio noudattaa muussa toiminnassaan selkeitä prosesseja, sitä enemmän kyberresilienssin hallintakeinoja sillä on käytössään. (Annarelli, Nonino & Palombi 2020, 13-17; Cyber Resilience Manager 2022.)

JOHTOPÄÄTÖKSET JA POHDINNAT

Artikkelissa on käsitelty kyberturvallisuutta riskienhallinnan, jatkuvuuden ja kyberresilienssin näkökulmasta. Hybridi- ja kybervaikuttamisen uhka Suomea kohtaan kasvaa koko ajan, jolloin varautuminen erilaisiin uhkiin korostuu. Riskienhallinnan ja jatkuvuuden perustyökaluilla voidaan hallita myös kyberturvallisuuden uhkia. Kyberturvallisuuden uhkat muuttuvat muita tyypillisiä jatkuvuuteen vaikuttavia uhkia useammin, organisaatioiden kannattaakin kiinnittää huomiota riskien arvioinnin ja tilannekuvan säännölliseen tarkastelemiseen ja päivittämiseen.

Riskienhallinta ja jatkuvuudenhallinta ovat tärkeä osa yrityksen turvallisuutta ja siihen pitää asennoitua oikein ja investoida turvallisuuteen ennen kuin jotain pahaa tapahtuu. Asiakkaita on vaikea saada, mutta ne on helppo menettää, jos yllättävän tietoturvapoikkeaman sattuessa ei osata toimia oikein ja hoitaa myös palautumista ja viestintää kunnolla. Yritystä ei auta se, että poikkeaman jälkeen yritys palautuu takaisin aiemmalle toimintatasolle, jos yritys on poikkeaman aikana menettänyt asiakaskantansa huonon kriisiviestinnän vuoksi. Kaikkeen ei toki voi varautua, joten riskejä pitää tunnistaa ja priorisoida, ja keskittyä jatkuvuussuunnittelussa niihin riskeihin, joiden torjunnasta yritys hyötyy eniten.

> ***Riskienhallinnan ja jatkuvuuden perustyökaluilla voidaan hallita myös kyberturvallisuuden uhkia.***

Kyberturvallisuuden resilienssi on jatkuvuudenhallinnan osa-alue, jonka tueksi on kehitetty erilaisia menetelmiä, jotka noudattelevat jatkuvuuden hallinnan perinteisiä menetelmiä, kuten Plan-Do-Check-Act-mallia. Kyberturvallisuuden osalta menetelmiin on otettu mukaan ketterästä kehittämisestä ja operointikehyksistä, kuten ITIL, tuttuja elementtejä, joissa tarkastellaan jälkikäteen prosessia ja tehtyjä toimenpiteitä.

Suuremmissa yrityksissä on tyypillisesti käytössä jonkinlainen projektikehityksen tai IT-operoinnin malli, jolloin kyberturvallisuuden resilisenssiä on helpompi hallita tällaisten mallien mukaisesti. Kyberresilienssiä ei saa irrottaa omaksi itsenäiseksi osakseen, vaan sen tulee olla sidoksissa organisaation kokonaisvaltaiseen kyberturvallisuuden riskien- ja jatkuvuudenhallintaan sekä tukea liiketoiminnan jatkuvuutta.

Riskienhallinta, kyberresilienssi ja jatkuvuussuunnittelu ovat niitä keskeisiä keinoja, joiden avulla voidaan vastata hybridi- ja kybervaikuttamisen tuomiin uhkiin.

Lähteet

Annarelli, A., Nonino, F. & Palombi, G. 2020. Understanding the management of cyber resilient systems. Computers & industrial engineering, 149,106829. Viitattu 3.4.2022. *https://doi:10.1016/j.cie.2020.106829*

Calder, A. 2020. ISO22301: 2019 - An introduction to a business continuity management system (BCMS). IT Governance Publishing. E-kirja.

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S. & Hernantes, J. 2020. Systematic Approach to Cyber Resilience Operationalization in SMEs. IEEE access, 8, 174200-174221.

Dionne, G. 2013. Risk Management: History, Definition and Critique. Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation. Viitattu 3.4.2022. *https://www.cirrelt.ca/documentstravail/cirrelt-2013-17.pdf*

Euroopan puolustus: komissio avaa keskustelun etenemisestä kohti turvallisuus- ja puolustusunionia 2017. Euroopan komissio. Lehdistötiedote. Viitattu 5.4.2022. *https://ec.europa.eu/commission/presscorner/api/files/document/print/fi/ip_17_1516/IP_17_1516_FI.pdf*

Finanssivalvonta 2022. Tehostettua seurantaa finanssisektorin tilanteeseen, pakotteiden toimeenpanoon ja kyberriskeihin varautumiseen. Viitattu 5.4.2022. *https://www.sttinfo.fi/tiedote/tehostettua-seurantaa-finanssisektorin-tilanteeseen-pakotteiden-toimeenpanoon-ja-kyberriskeihin-varautumiseen?publisherId=69817444&releaseId=69934186*

Herrman, H., Stewart, D.E., Diaz-Granados, N., Berger, E.L., Jackson, B., & Yuen, T. 2011. What Is Resilience? Canadian Journal of Psychiatry. 56(5), 258-265.

Hopkin, P. 2018. Fundamentals of Risk Management. Viides painos. Iso- Britannia: Kogan Page Limited.

Huoltovarmuuskeskus 2022. Sanasto. Viitattu 3.4.2022. *https://www.huoltovarmuuskeskus.fi/sanasto*

Isotalo, V. 2022. Kyberturvallisuus on riskienhallintaa. Viitattu 3.4.2022. *https://www.lounea.fi/yrityksille/artikkelit-ja-blogit/artikkelit-yritysasiakkaille/kyberturvallisuus-riskienhallintaa*

Kybersää helmikuu 2022 2022. Kyberturvallisuuskeskus. Viitattu 2.4.2022. *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20helmikuu%202022.pdf*

Kyberturvallisuuskeskus 2021. Tietoturvan selviytymispakki koteihin ja toimistoihin 3 uhkaa ja ratkaisua. Viitattu 3.4.2022. *https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-selviytymispakki-koteihin-ja-toimistoihin-3-uhkaa-ja-ratkaisua*

Lehto, M. 2021. Digitaalisen kybermaailman ilmiöitä ja määrittelyjä. Viitattu 5.4.2022. *https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kybma/kybermaailma_v15-0.pdf*

Maclean-Bristol, C. 2020. Business Continuity Exercises – Quick Exercises to Validate Your Plan. Rothstein Publishing. E-kirja.

Morgan, S. 2022. Cybercrime to cost the wordl 10.5 trillion annually by 2025. Cybercrime Magazine. Viitattu 3.4.2022. *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*

Niemimaa, M., Järveläinen, J., Heikkilä, M. & Heikkilä, J. 2019. Business continuity of business models: Evaluating the resilience of business models for contingencies. International journal of information management, 49, 208-216.

Rittinghouse, J. & Ransome, J. F. 2011. Business Continuity and Disaster Recovery for InfoSec Managers. Elsevier Science. E-kirja.

Ruoslahti, H. 2021. Resilienssi ja toiminnan jatkuvuus. Viitattu 5.4.2022. *http://urn.fi/URN:NBN:fi-fe202102053786*

ServiceNow™ 2022. What is business resilience? Viitattu 3.4.2022. *https://www.servicenow.com/products/governance-risk-and-compliance/what-is-business-resilience.html*

Swinfen Green, J. & Dorey, P. 2016. The Weakest Link. Bloomsbury Publishing. E-kirja.

Valtioneuvoston puolustusselonteko 2017. Valtioneuvoston kanslian julkaisusarja 5/2017. Viitattu 5.4.2022. *http://urn.fi/URN:ISBN:978-952-287-370-5*

Valtiovarainministeriö 2022. Ministerityöryhmä vastaamaan kyberturvallisuudesta ja julkisen hallinnon varautumisesta. Viitattu 5.4.2022. *https://vm.fi/-/ministerityoryhma-vastaamaan-kyberturvallisuudesta-ja-julkisen-hallinnon-varautumisesta*

Julkaisemattomat lähteet

Cyber Resilience Manager 2022. Haastattelu jatkuvuudenhallinnasta organisaatiossa 11.2.2022. Mediakonserni. Helsinki.

Jatkuvuudenhallinnan asiantuntija 2022. Haastattelu jatkuvuudenhallinnasta organisaatiossa 30.3.2022. ICT-alan pörssiyhtiö. Helsinki.Bor si aligniet erro quiam exerum fugit, estiis dolupta quis etur?Abo.


T
G
F
F
B

8 Kyberfyysisten järjestelmien resilienssin hallinta

Jyri Rajamäki

TURVALLISUUSINSINÖÖRIT OVAT LUONEET vuosikymmenten ajan strategioita kriittisen infrastruktuurin (energia, tietoliikenne, väylät, ym.) riskien poistamiseksi ja turvallisuuden lisäämiseksi. Nykyisin on yhä enemmän otettu käyttöön termi *resilienssi*, joka on monitahoinen vielä standardoimaton käsite sisältäen useita määritelmiä ja arviointimenetelmiä. Tähän asti *resilienssin hallinta* on keskittynyt pitkälti kuvaavaan tai diagnostiseen analytiikkaan asiantuntija-arviointiin perustuvan lähestymistavan mukaisesti.

Tämän artikkelin tarkoituksena on esitellä kriittisten kyberfyysisten järjestelmien resilienssin hallinnan käsite hyödyntäen kansainvälisistä HORIZONTI 2020 -projekteista saatuja oppeja. Tässä artikkelissa esitettävä lähestymistapa perustuu kyberluottamuksen käsitteen integrointiin kyberturvallisuustieteen ja resilienssitieteen kanssa. Artikkelissa ehdotetaan viittä periaatetta, jotka nousevat kyberfyysisten järjestelmien resilienssin hallintaprosessien teoriasta: (1) suunnitella ja toteuttaa turvallisuuden hallintasuunnitelma, (2) käyttää kaikkia asianmukaisia tietoturvatekniikoita, (3) varmistaa tietoturvatietojen riittävyys ja laatu, (4) varmistaa, että tilannetietoisuus on aina ajan tasalla, ja (5) suunnitella ja toteuttaa resilienssin hallintasuunnitelma, joka kattaa kaikki neljä tapahtumanhallintasykliä (suunnittele/valmistele, absorboi, toivu, mukaudu) ja keskinäiset riippuvuudet muiden järjestelmien kanssa.

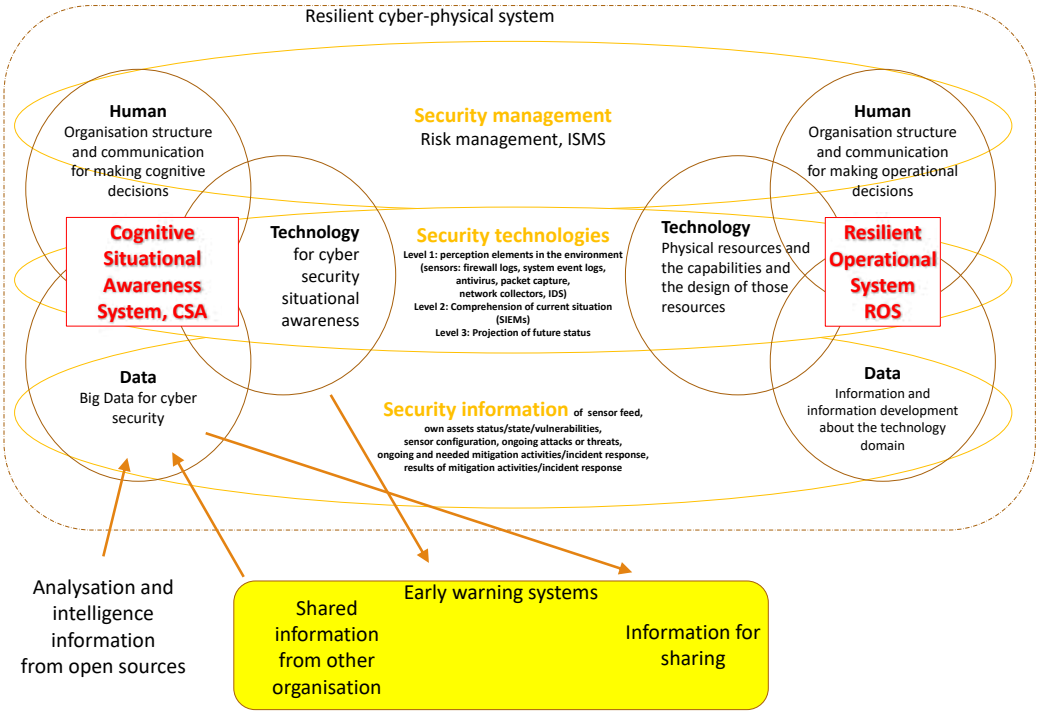
KYBERTURVALLISUUSTIETEEN INTEGROINTI KYBERLUOTTAMUKSEEN

Kuva 1 esittää kyberturvallisuustieteen kolme ulottuvuutta. Kaikista kyberfyysisistä järjestelmistä löytyvät sosiaalinen, teknologinen sekä ja informaation ulottuvuus. Sosiaalinen eli ihmisen näkökulma katsoo, että

sekä yksilöt että organisaatiot ovat yhtä vastuussa järjestelmän dynamiikasta kuin data ja tekniikka. Tämän näkökulman tieteellisen perustan antavat humanistiset sekä yhteiskuntatieteet. Insinööritieteisiin pohjautuva teknologianäkökulma sisältää niin laitteistot kuin ohjelmistot sisältäen muun muassa kaikki prosessoreja sisältävät laitteet, tietoliikenneyhteydet, käyttöjärjestelmät ja verkkoprotokollat. Tieto- tai informaationäkökulma käsittelee sekä ihmisten että teknologian tuottamaa tietoa pohjautuen tietojenkäsittely- ja informaatiotieteisiin. (Edgar & Manz 2017.)

Kuvio 1. *Kyberturvallisuustieteen ulottuvuudet, muokattu (Edgar & Manz, 2017).*

Kuvio 2 esittää resilientin kyberfyysisen järjestelmän periaatteen, joka koostuu kahdesta alijärjestelmästä: varsinaisesta operationaalisesta järjestelmästä (Resiliens operational system, ROS) sekä kognitiivisesta tilannetietoisuusjärjestelmästä (Cognitive situational awareness system, CSAS). Molemmilla alijärjestelmillä on kuvan 1 mukaisesti ihmisen (sosiaalinen), teknologian (fyysinen) ja datan (informaatio) ulottuvuudet.



Kuva 2. *Kyberfyysisen järjestelmän kyberturvallisuuden konseptimalli.*

Turvallisuuden hallinta, turvallisuusteknologiat ja *tietoturvatiedot* yhdistävät edellä esitetyt alijärjestelmät toisiinsa. Turvallisuuden hallinta kattaa kyberturvallisuuden inhimilliset ja organisatoriset näkökohdat. Samalla se integroi sosiaalisen kerroksen toiminnalliset ja kognitiiviset näkökohdat toisiinsa.

Turvallisuusteknologioita käytetään viiteen päätarkoitukseen. Ensinnäkin rakennetaan operatiivinen järjestelmä turvallisemmaksi käyttää. Toiseksi muodostetaan lisäsuojausta operatiivisen järjestelmän ympärille. Kolmanneksi luodaan turvallisuustietoa joko operatiivisesta järjestelmästä, suojausjärjestelmistä tai kyseisen kyberfyysisen järjestelmän ulkopuolelta. Neljänneksi niitä käytetään turvallisuustiedon siirtämiseen sekä turvallisuustietämyksen vaihtoon. Niillä myös muodostetaan tilannetietoisuus ja visualisoidaan se päätöksenteon tueksi.

Turvallisuustietoa tarvitaan tilannetietoisuuden rakentamiseksi. Sitä luodaan operatiivisesta järjestelmästä ja tämän suojauksesta. Osa turvallisuustiedosta saadaan operatiivisen järjestelmän ulkopuolelta joko avoimista lähteistä (open source intelligence, OSINT) tai eri järjestelmien välisen tietojenvaihdon avulla (esim. early warning systems).

KOGNITIIVINEN PÄÄTÖKSENTEKOPROSESSI

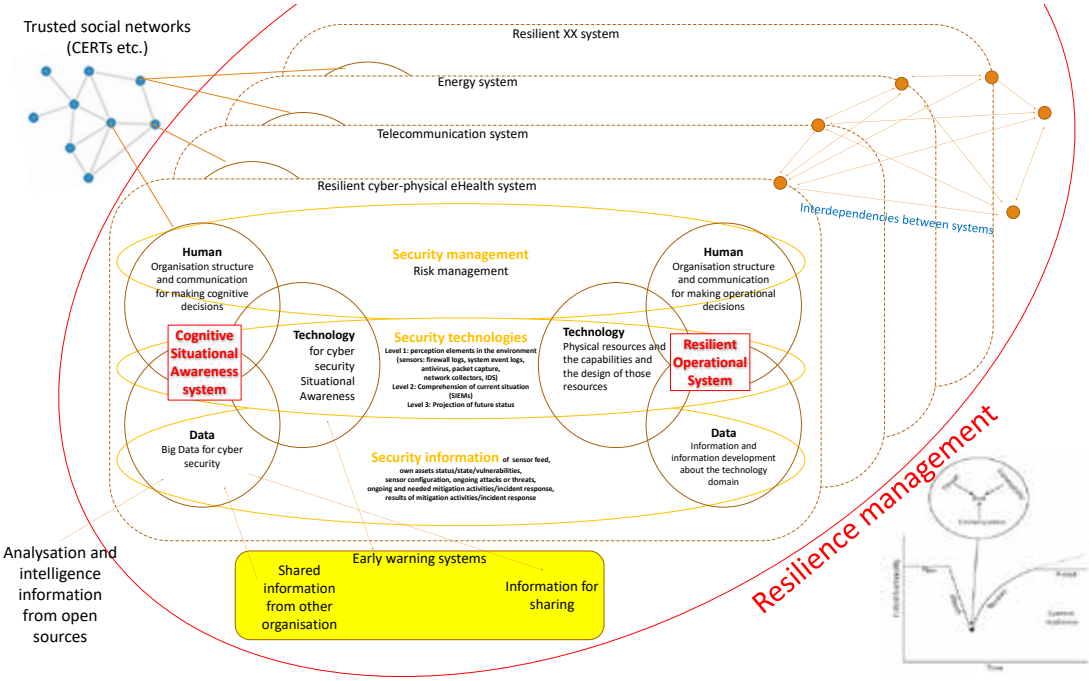
CSAS-järjestelmän teknologia-alue sisältää datafuusiomoottorin, tietorajapinnat ja tehokkaan visualisointikerroksen muodostavan ihmisen ja koneen välisen rajapinnan (*human-machine interface, HMI*) (Kokkonen 2016). Nykyaikaisten tehokkaiden kognitiivisten päätöksentekotoimintojen tulee hyödyntää tekoälyä ja olla mahdollisimman automaattisia ilman ihmisen vuorovaikutusta (Rajamäki 2021). Kuitenkin tarvitaan operaattori, joka ohjaa antureita ja datafuusioalgoritmeja ja syöttää lisätietoa järjestelmään. Järjestelmä toteuttaa HMI:n hallittavan kybertoimialueen tilan tehokkaaseen visualisointiin ja sellaisten tietojen syöttämiseen, joita ei voida syöttää automaattisesti. Ihmisiä tarvitaan ohjaamaan datafuusioprosessia ja tekemään päätöksiä. HMI:n tulee toteuttaa erilaisia visualisointeja eri käyttäjätasoille: esim. tekninen käyttäjä, joka tarvitsee yksityiskohtaista teknistä tietoa, kun taas päätöksentekijä tarvitsee erilaisen visualisoinnin. HMI toteuttaa myös suodattimia eri käyttäjille sallituille tiedoille.

Kuvion 2 kognitiivinen tilannetietojärjestelmä hyödyntää operatiivisen järjestelmän tietoja tehdäkseen parempia resilienssiin tähtääviä päätöksiä. Kognitiivisessa päätöksentekoprosessissa hyödynnetään kyberturvallisuusanturitietoa sekä kaikkien tunnettujen kyberolioiden tilatietoja. Tiedot järjestelmistä, laitteista ja antureista tila- ja konfiguraatiotietoineen, mutta myös tiedot fyysisten laitteiden käytetyistä varaosista ovat olennaista tietoa CSAS-järjestelmälle (Kokkonen 2016). Lisäksi tulee raportoida tiedot tallennettujen tietojen tilasta ja tietovirtojen tilasta. Osa tiedoista voidaan tuottaa automaattisesti tietoliitäntöjen avulla, ja osa pitäisi olla käyttäjän luomia käyttöliittymän avulla.

Kognitiivinen päätöksentekoprosessi edellyttää myös tiedonvaihtoa eri sidosryhmien välillä sekä avoimista lähteistä peräisin olevaa dataa, kuten kuvan 4 alaosasta näkyy. Varhaisvaroitusjärjestelmät toteuttavat rajapintoja kyberturvallisuuden tiedonvaihtoon luotettujen kumppaneiden kanssa. Lisäksi CSAS tarvitsee analyysi- ja tiedustelutietoa avoimista lähteistä. Tällaiset tiedot sisältävät analysoituja vaikutustenarviointitietoja (*Indicator of Compromise, IOC*) ja ennakkovaroitustietoja avoimen lähdekoodin tiedustelupalveluista esimerkiksi sosiaalisen median tai CERT (*Computer Emergency Response Team*) -tiedotteiden avulla. Lisäksi vaaditut politiikat ja tavoitteet tulisi syöttää järjestelmään.

RESILIENSSIN HALLINTAKEHYS

Kuvio 3 esittää resilientin kyberfyysisen järjestelmän hallintakehyksen. Se perustuu edellä esitettyyn yhden järjestelmän kyberturvallisuusmalliin (kuva 2) sekä liitäntöihin muiden kyberfyysisten järjestelmien kanssa. Kuusi tärkeää kyberturvallisuuden ja -resilienssin teemaa ovat: resilientit operatiiviset järjestelmät, turvallisuuden hallinta, turvallisuusteknologiat, turvallisuuteen liittyvä tieto, kognitiivinen tilannetietoisuus ja resilienssin hallinta. Johtamiskehyksen tavoitteena on toimintajärjestelmän resilienssin ylläpito, joka saavutetaan viiden muun teeman kautta. Seuraavaksi tarkastellaan periaatteet näiden teemojen käsittelemiseen.



Kuvio 3. *Kyberfyysisen järjestelmän resilienssin konseptimalli*

Periaate 1: Suunnittele ja toteuta turvallisuusjohtamissuunnitelma:

- huolehdi kyberriskien hallinta,
- tunnista ja koordinoi ulkoisia tahoja, jotka voivat vaikuttaa sisäisiin kyberhyökkäyksiin tai joihin ne voivat vaikuttaa (perusta yhteyspiste),
- kouluta ja harjoita työntekijöitä kyberturvallisuudesta ja organisaation turvallisuusjohtamissuunnitelmasta,
- valtuuta kaikki kilpailuvaltit ja palvelut tietyille työntekijöille,
- valmistele turvallisuusviestintää,
- luo kybertietoisuuden kulttuuri.

Periaate 2: Käytä kaikkia asianmukaisia suojatekniikoita:

- implementoi kontrollit ja sensorit kaikkiin kriittisiin kilpailuvaltteihin sekä palveluihin
- määritä verkon rakenne ja yhteenliittymät järjestelmäkomponentteihin ja ympäristöön
- toteuta kriittisen fyysisen infrastruktuurin redundanssi
- määritä verkosta fyysisesti tai loogisesti erotettujen tietojen redundanssi.

Periaate 3: Turvatietojen riittävyyden ja laadun varmistaminen:

- varmista tietojen soveltuvuus tekoälyn ja koneoppimistekniikoiden hyödynnettäviksi,
- luokittele kilpailuvaltit ja palvelut herkkyyden perusteella,
- tallenna kriittisten laitteisto- ja/tai ohjelmistotoimittajien sertifikaatit ja pätevyydet,
- laadi suunnitelmat turvaluokiteltujen tai arkaluonteisten tietojen säilyttämiseksi ja hallitsemiseksi,
- tunnista sisäiset järjestelmäriippuvuudet.

Periaate 4: Varmista, että tilannetietoisuus on aina ajan tasalla:

- ennakoi ja suunnittele järjestelmän tilat ja tapahtumat,
- ymmärrä organisaation tavoitteiden suorituskyvyn tasapaino,
- perusta skenaariopohjainen kybersotapeli,
- käytä soveltuvia järjestelmän tilan suunnitelmia, kun ne ovat saatavilla,
- hyödynnä tekoälyä tai valmistaudu sen käyttöön uhkiin vastaamisessa entistä varmemmin ja nopeammin.

Periaate 5: Suunnittele ja toteuta resilienssin hallintasuunnitelma, joka kattaa kaikki neljä tapahtumanhallintasykliä (suunnittele/valmistele, absorboi, toivu, mukauta) ja keskinäiset riippuvuudet muiden järjestelmien kanssa:

- pohdi kuinka kaikkia aikaisempia vaatimuksia voidaan hyödyntää neljän tapahtumanhallintasyklin aikana
- tunnista ulkoiset järjestelmäriippuvuudet (eli tietoliikenne, energia, rakennettu ympäristö) ja suunnitella koordinointikehys näiden järjestelmien kanssa (sinulla ei ole hallintaa näihin järjestelmiin)
- kouluta ja harjoituta työntekijät resilienssiajatteluun sekä organisaation resilienssisuunnitelmaan.

JOHTOPÄÄTÖKSET

Tämä artikkeli tarjoaa käsitemallin kyberfyysisten järjestelmien resilienssin hallintaan. Mallin pohjalta voidaan havaita viisi resilienssin hallinnan periaatetta. Ensimmäinen periaate ”suunnittele ja toteuta turvallisuusjohtamissuunnitelma” perustuu perinteiselle turvallisuusjohtamisperinteelle. Sen oletuksena on, että olemme turvassa ja meidän on suunniteltava, kuinka suojautua ulkopuolelta tulevilta uhilta riskienhallinnan avulla. Toinen periaate ”käytä kaikkia asianmukaisia turvatekniikoita” jatkaa tätä perinnettä ja tarjoaa työkaluja suojaukseen.

Kolmas periaate ”turvatietojen riittävyyden ja laadun varmistaminen” tarkoittaa, että tarvitsemme tietoja järjestelmäsi ymmärtämiseen, päätöksenteon tietotarpeiden ymmärtämiseen ja tällaisten päätösten tukemiseen tarvittavan tiedon valitsemiseen/tuottamiseen. Neljäs periaate ”varmista, että tilannetietoisuus on aina ajan tasalla” tarkoittaa, että edellä mainitut tiedot on muutettava päätöksentekoa tukevaksi tiedoksi.

Viides periaate ”suunnittele ja toteuta resilienssin hallintasuunnitelma” menee pidemmälle kuin perinteinen riskienhallintaan perustuva tietoturvan hallinta. Kukaan ei voi yksin kontrolloida ja suojata infrastruktuurijärjestelmä, kun vakavia tapauksia, kuten COVID-19-pandemia, tapahtuu joka tapauksessa. Reslienssin hallinnassa organisaation tulee tuntea kriittisimmät kilpailuvaltit ja palvelut sekä huolehtia niiden kriittinen toimintakyky kaikissa mahdollisissa olosuhteissa, kuten ihmiskeho pyrkii huolehtimaan sydämen ja aivojen toiminnasta viimeiseen asti.

Riskien hallinta on yritysten ja muiden organisaatioiden nykypäivää ja siihen on olemassa useita erilaisia työkaluja. Yllä esitetyt viisi resilienssin hallinnan periaatetta on johdettu yhdistämällä eri teorioita, mutta käytännön toteutuksia ei juurikaan ole. Jatkossa tulisikin kehittää menetelmiä ja työkaluja resilienssin hallintaan.

Lähteet

Edgar, T., & Manz, D. 2017. Research methods for cybersecurity. Cambridge: Syngress.

Kokkonen, T. 2016. Anomaly-Based Online Intrusion Detection System as a Sensor for Cybersecurity Situational Awareness System. Jyväskylä studies in computing 251. University of Jyväskylä. *http://urn.fi/URN:ISBN:978-951-39-6832-8*

Rajamäki, J., 2021. Resilience Management Concept for Railways and Metro Cyber-Physical Systems. Teoksessa: T. Eze, toim. Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS . Reading: Academic Conferences International Limited, pp. 337-345.

9 "Critical Entities Resilience"-direktiivin vaikutus kansalliseen varautumiseen

Lauri Halonen, Juho Jokinen, Tomi Koskela, Ville Savolainen, Juha Takala & Paula Ylhäinen

JOHDANTO

TÄMÄ ARTIKKELI ON tehty osana Laurea-ammattikorkeakoulun Turvallisuusjohtamisen YAMK-tutkinnon opintojaksoa "Toiminnan jatkuvuuden varmistaminen". Artikkeli käsittelee "critical entities resilience"-direktiivin (CER-direktiivi) vaikutuksia nykyiseen lainsäädäntöön ja toimintatapoihin. Artikkelin tavoite on selvittää Suomen viranomaisjohtoisen varautumisen nykytila ja arvioida CER-direktiivin toimeenpanon mahdollisia vaikutuksia siihen.

Vuonna 2020 esitelty ja lähitulevaisuudessa toimeenpantava Euroopan Parlamentin ja neuvoston direktiivi kriittisten toimijoiden häiriönsietokyvystä (Critical Entities Resilience, jatkossa CER-direktiivi) tulee uudistamaan Euroopan Unionin jäsenmaiden viranomaisten varautumismenettelyä. Direktiivin avulla pyritään reagoimaan muuttuneen toimintaympäristön muodostamiin uusiin uhkiin, kuten EU:n sisämarkkinoilla toimivien palveluiden lisääntyneeseen keskinäisriippuvuuteen ja teknologian mahdollistamaan valtiolähtöiseen vihamieliseen toimintaan. Euroopan komissio on tunnistanut rajat ylittävien häiriöiden merkityksen koko Euroopan turvallisuudelle ja esittää direktiivissä jäsenmaille yhtenäisiä lähestymistapoja näiden hallitsemiseksi. CER-direktiivi tulee korvaamaan vanhentuneen kriittistä infrastruktuuria suojaavan direktiivin 2008/114EC ja laajentaa soveltamisalaa merkittävästi, koskemaan yhteensä kymmentä sektoria. CER-direktiivi (kuten kaikki direktiivit) on lainsäädäntöohje, jota ei sellaisenaan oteta osaksi kansallista lainsäädäntöä, vaan jonka pohjalta kansallinen lainsäädäntö tulee saattaa direktiiviä vastaavaksi. CER:n voimaantulon oletetaan edellyttävän jäsenmailta merkittäviä toimia kansallisen varautumisen edistämiseksi. (Euroopan komissio 2020, 1–3.)

Suomessa merkittävin yhteiskunnan varautumista ohjaava asiakirja on yhteiskunnan turvallisuusstrategia (jatkossa YTS), joka kuvaa kansallisen varautumisen keskeiset prosessit ja vastuut sekä ohjaa eri hallinnonalojen varautumista. (Turvallisuuskomitea 2017, 5–7.) Kyseinen, vuonna 2017 julkaistu valtioneuvoston periaatepäätös eroaa CER-direktiivistä sekä rakenteeltaan että kohderyhmältään: YTS ohjaa ensisijaisesti kansallisten viranomaisten roolia elintärkeiden toimintojen ylläpitämisessä, CER puolestaan ohjaa määrittelemään sektorikohtaiset kriittiset toimijat riippumatta siitä ovatko nämä yksityisiä vai julkisia. Yksityisten toimijoiden varautumisen julkinen ohjaus ja valvonta vaatinee lainsäädäntömuutoksia, joten tarkastelemme artikkelissamme lyhyesti myös muita tämänhetkisiä säädöksiä sekä pohdimme niiden mahdollisuuksia CER-direktiivin toimeenpanon tukena.

Valtioneuvosto on lausunut tukevansa CER-direktiivin tavoitteita ja jakavansa komission käsityksen kriisinkestävyyden kokonaisvaltaisen kehittämisen tärkeydestä. Lausuntoa tukee myös heidän toimintansa, sillä CER:n vaatimia keskeisiä toimia kuten kansallista riskienarviointia, systemaattista kriittisten toimijoiden tunnistamista ja kansallisen strategian laatimista on Suomessa tehty jo vuosia. Lähtökohdat uuden direktiivin käyttöönotolle ovat paremmat kuin monessa muussa EU-maassa, mutta siinä esitetyn tavoitetilan saavuttaminen edellyttää arviomme mukaan huoltovarmuusjärjestelmämme mukauttamista ja entistä laajempaa viranomaisohjausta sekä -valvontaa. (Eduskunta 2020.)

Tämä artikkeli perehtyy CER:n vaikutuksiin yhteiskuntamme varautumiseen kuvailevan kirjallisuuskatsauksen avulla. Käytetty aineisto on rajattu julkisiin viranomaislähteisiin: Nykytilaa on arvioitu yhteiskunnan turvallisuusstrategian lisäksi sen taustalla vaikuttavien lakien, asetusten ja viranomaismääräysten avulla. CER-direktiivin osalta tutkimus tukeutuu säädösprosessin valmisteluasiakirjoihin, kansallisten viranomaisten muistioihin ja lausuntoihin sekä viranomaisinstituutioissa toimivien asiantuntijoiden julkaisuihin. Aineistolle on suoritettu sisällönanalyysi teemoittelemalla.

CER-DIREKTIIVIN VAIKUTUKSET NYKYTILAAN

Varautumisen säädösperusta ja muu ohjaava dokumentaatio

Suomen julkishallinnon toimijoille on asetettu varautumisvelvollisuus Valmiuslain (1552/2011) 12 §:ssä. Osalle julkishallinnon toimijoista varautumisvelvollisuutta on tarkennettu muilla säädöksillä, kuten Pelastustoimelle pelastuslaissa (379/2011) ja Valtorille laissa valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (1226/2013). Tiedonhallintalaki edellyttää julkishallinnon toimijan tietohallinnolta ajantasaisia ohjeita poikkeusoloihin varautumisesta tiedonhallinnan näkökulmasta (906/2019, 4 §).

Suomen yhteiskunnan varautumisen yhteiset periaatteet määritellään Yhteiskunnan turvallisuusstrategiassa. Tuorein Yhteiskunnan turvallisuusstrategia on vuodelta 2017. Ensimmäisen kerran strategia valmistui vuonna 2003 nimellä ”Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia”, jota päivitettiin vuonna 2006. Vuosina 2010 ja 2017 julkaistut version on nimetty “Yhteiskunnan turvallisuusstrategiaksi”. (Turvallisuuskomitea 2017, 5.)

Yhteiskunnan turvallisuusstrategia on luonteeltaan ohjaava asiakirja ja se jalkautetaan alemman tason strategioissa (hallinnonalakohtaiset strategiat, poikkihallinnolliset strategiat, toimeenpano-ohjelmat jne.). Dokumentin ajanmukaisuuden/vastaavuuden seurannasta on vastuussa Turvallisuuskomitea ja sitä päivitetään valtioneuvoston päätöksellä tarpeen mukaan. (Turvallisuuskomitea 2017, 7.)

Yhteiskunnan turvallisuusstrategia ei ole juridisesti sitova määräys, vaan valtioneuvoston periaatepäätös. Vaikka dokumentti varsin ymmärrettävästi pyrkii jatkuvuuteen yli vaalikausien, se ei ole määräävä asiakirja, vaan poliittinen kannanotto, joka sitoo korkeintaan sen hyväksynyttä hallitusta. (Valtioneuvosto 2022.)

Riskiarviointi

Yhteiskunnan turvallisuusstrategia edellyttää, että varautumisen tulee perustua jatkuvaan riskiarvioon, joka ottaa huomioon kaikki uhkamallit. YTS:ssä esitelty riskiarvio on tulosta vuonna 2015 tehtyyn, poikkihallinnollisesti toteutettuun kansalliseen riskiarvioon ja vuonna 2010 julkaistun Yhteiskunnan turvallisuusstrategian uhka-arviointeihin. (Turvallisuuskomitea 2017, 25.)

CER-direktiivin 10. artiklassa velvoitetaan kriittiset toimijat tekemään riskiarviointi kaikista niiden toiminnalle merkityksellisistä riskeistä. Riskiarvio pohjautuu jäsenvaltioilta saatuun riskiarviointiin sekä muihin asiaan liittyviin tietolähteisiin. Riskiarviointi tulee tehdä kuuden kuukauden kuluessa siitä, kun organisaatiolle on muodollisesti ilmoitettu heidän olevan huoltovarmuuskriittinen organisaatio vastaavan viranomaisen toimesta. Riskit tulee arvioida vähintään neljän vuoden välein. Riskiarvioinnissa on käsiteltävä direktiivin 4. artiklan 1. kohdassa mukaisesti kaikkia merkityksellisiä luonnonriskejä ja ihmisen aiheuttamia riskejä, jotka voivat aiheuttaa häiriöitä keskeisten palvelujen tarjoamisessa mukaan lukien onnettomuudet, luonnonkatastrofit, kansanterveysuhat ja vihamieliset uhat, kuten Euroopan parlamentin ja neuvoston direktiivissä (EU) 2017/54134 tarkoitetut terrorismirikokset. (Euroopan komissio 2020, 25–26, 29.)

Riskiarvioinnissa on otettava huomioon direktiivin liitteessä mainittujen toimialojen mahdollinen riippuvuus kriittisen toimijan tarjoamasta keskeisestä palvelusta, tapauksen mukaan myös naapurijäsenvaltiossa sekä kolmansissa maissa. Lisäksi tulee huomioida ne vaikutukset kriittisen toimijan tarjoamaan keskeiseen palveluun, jotka johtuvat keskeisten palvelujen tuottamisen häiriintymisellä yhdellä tai useammalla toimialalla. (Euroopan komissio 2020, 29.)

Kriittiset toimijat

Yhteiskunnan turvallisuusstrategia määrittelee seitsemän yhteiskunnan toimivuuden kannalta välttämätöntä toimintakokonaisuutta, joiden alle kriittiset julkishallinnolliset toimijat on määritelty: Johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri, huoltovarmuus, väestön toimintakyky ja palvelut ja henkinen kriisinkestävyys (Turvallisuuskomitea 2017, 14).

Johtamisen osalta painotetaan johtamiskyvyn turvaamista kaikissa tilanteissa kaikilla tasoilla ja se edellyttää tilannekuvan ylläpitoa, selkeyttä johtovastuiden osalta ja yhteistoimintaa kaikkien turvallisuustoimijoiden kesken. Kansainvälinen ja EU-toiminta kohdassa korostetaan EU-turvallisuusyhteistyötä ja osallistumista EU:n päätöksentekoon. Puolustuskyvyn tarkoitus on muodostaa ennaltaehkäisevä kynnys sotilaallisen voiman käytölle Suomea vastaan, varmistaa alueellinen koskemattomuus ja torjua sotilaalliset uhat sotilaallisia voimakeinoja käyttäen. Puolustuskyvyn osalta päätoimija on puolustusvoimat.

Sisäisen turvallisuuden ylläpitäminen ennaltaehkäisee Suomeen tai suomalaisiin kohdistuvia rikoksia, onnettomuuksia ja ympäristövahinkoja. Sisäisen turvallisuuden osalta vastuuviranomaisia on lukuisia; poliisi, pelastuslaitos, rajavartiolaitos, sosiaali- ja terveydenhuolto jne. Talous, infrastruktuuri ja huoltovarmuus pyrkii varmistamaan rahoitusmarkkinoiden toimivuuden, elintarvikehuollon, energiansaannin infrastruktuurin jne. toimivuuden – eritoten elinkeinoelämän merkitys korostuu tässä kohdassa. Väestön toimintakyky ja sen ylläpitäminen edellyttää sekä kiireellisten palvelujen (terveydenhuolto, sosiaalitoimi jne.) että ns. kiireettömien palvelujen (koulutus jne.) toimivuutta kaikissa olosuhteissa.

Viimeisenä kohtana mainitaan henkinen kriisinkestävyys, joka edistää kriiseissä toimimista ja kriiseistä toipumista. Se ilmenee tahtona toimia yhteiskunnan eduksi – henkisen kriisinkestävyyden avulla yhteiskunta voi selvitä yli haastavista ajoista. Tässä kohtaa normaalioloissa luotu luottamus viranomaisiin on ratkaiseva tekijä. (Turvallisuuskomitea 2017, 17–26).

CER-direktiivin soveltamisalaan kuuluu kymmenen sektoria: Liikenne, energia, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveydenhuolto, juomavesi- ja jätevesihuolto, digitaalinen infrastruktuuri, julkishallinto ja avaruus (Euroopan komissio 3.). Suomen huoltovarmuusmallin ja CER-direktiivin sisällön keskeisin eroavaisuus on toisistaan poikkeava määritelmä oleellisista sektoreista. CER- direktiivi kattaa 10 sektoria, jotka asettuvat Suomen kannalta yhteiskunnan elintärkeiden toimintojen ja huoltovarmuuden turvaamiseksi tunnistettujen sektorien ja toimialojen väliin. Direktiivissä mainittujen julkishallinnon ja avaruuden osalta ei löydy suoraa kytköstä huoltovarmuuden kannalta keskeisistä sektoreista tai toimialoista. (Huoltovarmuuskeskus 2021.)

CER-direktiivin 5. artikla (Euroopan komissio 2020, 26.) määrittelee soveltamisalaan kuuluviksi kriittisiksi toimijoiksi sellaiset toimijat, jotka täyttävät seuraavat vähimmäisvaatimukset: toimija tarjoaa yhtä tai useampaa keskeistä palvelua jäsenmaassa, kyseisen palvelun tarjoaminen on riippuvainen jäsenvaltiossa sijaitsevasta infrastruktuurista ja toimijaan kohdistuvalla poikkeamalla olisi merkittäviä haitallisia vaikutuksia joko kyseisen palvelun tarjoamiseen tai kyseisestä palvelusta riippuvaisten toimijoiden toimintaan. Suomen huoltovarmuuden kannalta kriittiset sektorit ja toimialat määritellään valtioneuvoksen päätöksessä huoltovarmuuden tavoitteista (1048/2018). Sen rooli on vastaavanlainen kuin CER-direktiivin 3. artiklassa mainittu kansallinen strategia kriittisten toimijoiden häiriösietokyvyn vahvistamiseksi. (Huoltovarmuuskeskus 2021; Euroopan komissio 2020, 24.)

Turvallisuusselvitykset

Kriittisten toimijoiden häiriönsietokyvystä tehdyn direktiiviehdotuksen 12 artiklassa on ehdotettu, että EU jäsenvaltioiden tulee varmistaa, että kriittisten toimijoiden palvelukseen harkittavista henkilöistä voidaan tehdä taustatarkistukset ja näihin tarkistuspyyntöihin tulee vastata nopeasti. Palvelukseen harkittavista henkilöistä voitaisiin tehdä selvitys henkilöllisyyden varmentamisesta, rikosrekisteristä ja koulutus- ja työhistoriasta. (Euroopan komissio 2020, 32.)

Rikosrekisteritietojen osalta kriittiset toimijat saisivat direktiiviehdotuksen mukaan vähintään viideltä edeltävältä vuodelta ja enintään kymmenen vuoden ajalta tiedot sellaisten rikosten osalta, joilla on merkitystä palvelukseen otossa tiettyyn tehtävään. Tiedot saataisiin myös henkilöstä, joka on asunut viimeisen kymmenen vuoden aikana EU jäsenvaltiossa tai kolmannessa maassa. (Euroopan komissio 2020, 32.)

Sisäministeriön muistiossa 21.1.2021 EU/2020/1795 on tuotu esille, että direktiiviehdotuksen läpimeno vaatisi Suomen lainsäädännön muutoksia turvallisuusselvityslakiin (726/2014) ja lakiin henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). Sisäministeriön muistion mukaan EU-rikosrekisteritietoja ei voida nykyisen kansallisen lainsäädännön puitteissa luovuttaa suppeiden turvallisuusselvitysten osalta, minkä piiriin osa tarkistuksen kohteena olevista henkilöistä tulisivat kuulumaan. (Sisäministeriö 2021, 12.)

Suomessa henkilöturvallisuusselvitysten ja yritysturvallisuusselvitysten tekemisen osalta toimivaltainen viranomainen on suojelupoliisi. Lisäksi puolustusvoimien pääesikunta liittyen puolustusvoimien toimintaan tai hankintoihin. (Turvallisuusselvityslaki 726/2014, 3 luku 9§.) Euroopan unionin neuvoston puitepäätöksen 2009/315/YOS artiklan 3 kohdan 1 mukaan jokaisen EU jäsenvaltion tulee varmistaa, että kaikkien rekisteröitävien tuomioiden osalta rekisterissä on tieto myös tuomitun kansalaisuudesta tai kansalaisuuksista, jos kyseessä on jonkin toisen valtion kansalainen. Suomessa oikeusministeriön hallinnonalan rekisterinpitäjänä on oikeusrekisterikeskus (Laki oikeusrekisterikeskuksesta 625/2012).

Suomen oikeusministeriö on valmistelemassa hallituksen esitystä ECRIS-TCN-asetusta täydentäväksi lainsäädännöksi ja ECRIS-TCN-direktiivin täytäntöönpanolainsäädännöksi. ECRIS on eurooppalainen rikosrekisteritietojärjestelmä, joka koostuu EU jäsenmaiden ulkopuolisten maiden kansalaisille annetuista rikostuomioista. Keskitetty järjestelmä mahdollistaa tietojenvaihdon EU:ssa annetuista rikostuomioista jäsenmaiden kesken. (Oikeusministeriö 2021.) Suomen kansallinen lainsäädäntö ECRIS-TCN-direktiiviin liittyen on säädettävä, jotta Suomi voi täyttää CER-direktiivin 12 artiklassa suunnitellut jäsenvaltioiden velvoitteet luovuttaa rikosrekisteritietoja eurooppalaisen rikosrekisteritietojärjestelmän kautta sekä tehdä hakuja tiedoista koskien kolmannen maan kansalaisten tuomioita. (Oikeusministeriö 2021.)

EU-rikosrekisteritietoja ei voida nykyisen lainsäädännön puitteissa sisällyttää luovutettaviin tietoihin, kun selvityksen kohteena on henkilö, joka kansallisen lainsäädännön mukaan kuuluu suppean turvallisuusselvityksen piiriin (Sisäministeriö 2021, 12). Artiklan 12 2b kohta koskee rikosrekisteritietoja vähintään viiden edeltävän vuoden ajalta ja enintään kymmenen vuoden ajalta rikoksista henkilön kansallisuusjäsenvaltiossa tai -valtioissa sekä muussa jäsenvaltiossa tai kolmannessa maassa, jossa henkilö on asunut kyseisenä aikana. (Euroopan komissio 2020, 31.) Suomen turvallisuusselvityslain (726/2014) 30 ja 25 §:n mukaisesti suppean turvallisuusselvityksen piirin kuuluvasta henkilöstä ei voida nykyisen kansallisen lainsäädännön puitteissa hakea tietoja toisen valtion viranomaisten pitämistä rikosrekisteri- tai sakkorekisteritiedoista.

Ilmoitusvelvollisuus

Poikkeamailmoituksista säädetään CER-direktiivin 13. artiklassa. Huoltovarmuuskriittisen organisaation tulee ilmoittaa ilman aiheetonta viivytystä viranomaiselle poikkeamista, jotka voivat häiritä muiden huoltovarmuuskriittisten toimijoiden toimintaa. Poikkeamailmoituksen yhteydessä on arvioitava häiriön vaikutusten alaisten käyttäjien määrä, häiriön kesto sekä häiriön maantieteellinen alue. Toimivaltainen viranomainen on velvollinen antamaan kriittiselle toimijalle poikkeamailmoituksen jälkeen toimintaohjeita sekä sellaisia tietoja, jotka voivat tukea kriittistä toimijaa poikkeamaan reagoimisessa. (Euroopan komissio 2020, 31–32.)

Ilmoitettuja poikkeamia hyödynnetään jäsenvaltioiden tekemissä riskiarvioissa ja kansallisten kriittisten toimijoiden sekä Euroopan unionin jäsenvaltioiden varautumisen toimivaltaisten viranomaisten keskinäisessä kommunikaatiossa. (Euroopan komissio 2020, 25–28.)

Sanktiointi

Valmiuslaissa ei ole säädetty rangaistusta varautumisvelvollisuuden rikkomisesta. Valmiuslain rangaistussäännökset koskevat valmiuslailla käyttöönotettujen poikkeussäädöksien, kuten ulkonaliikkumiskiellon ja säännöstelyn, rikkomisesta aiheutuvia rangaistuksia. (Valmiuslaki 1552/2011, 132–133 §.)

CER-direktiivi asettaa sanktioinnin varautumisvelvollisuuden rikkomisesta. CER-direktiivin 19 artiklassa määritellään direktiivissä asetettujen vaatimuksien rikkomisesta aiheutuvat seuraamukset. Artiklassa edellytetään seuraamuksilta tehokkuutta, oikeasuhtaisuutta sekä varoittavuutta. (Euroopan komissio 2020, 36.)

POHDINTA

CER-direktiivi vastaa Suomen nykymallia pääpiirteissään hyvin, vaikka yksittäisiä muutoksia direktiivin mukana tuleekin.

Yhteiskunnan turvallisuusstrategia lähestyy yhteiskunnan varautumista kokonaisturvallisuuden yhteistoimintamallin kautta, jossa jokaisella toimijalla (viranomaiset, järjestöt, elinkeinoelämä ja kansalaiset) on omat vastuualueensa ja jossa toimijat ovat oikeasti yhteistyössä keskenään. Vuoden 2017 versio painottaa yhteisen ja yleisen varautumisen periaatteita ja merkittävä painotusero aiempaan on, että turvallisuustoimijat toimivat oikeasti yhteistyössä. CER-direktiivi tavoittelee samaa asiaa lainsäätämisen kautta.

Yhteiskunnan turvallisuusstrategia 2017 ei keskity pelkästään valtiotason toimintaan, vaan koko turvallisuuskenttään (sisältäen elinkeinoelämän, järjestöt ja kansalaiset ja niin edelleen). Modernissa yhteiskunnassa elinkeinoelämän varautumisvelvollisuudet ovat merkittävästi kasvaneet, eritoten (edes osittain) julkista tehtävää suorittavilla yksityisillä yrityksillä (esim. ulkoistetut sosiaali- ja terveyshuollon palvelut). Näin ollen CER-direktiivin mukanaan tuoma tiukempi varautumiseen liittyvä lainsäädäntö on tarpeellinen.

Säädökset

Moniin muihin Euroopan unionin maihin verrattuna Suomen huoltovarmuusjärjestelmä on edelläkävijän asemassa. Huoltovarmuuskriittisiä toimijoita koskevassa sääntelyssä on kuitenkin tarkennettavaa. Valmiuslaissa määritetään varautumisvelvollisuus ja YTS:ssä asetetaan varautuminen perustuvaksi riskienhallinnalle, mutta näitä vaatimuksia syventävää lainsäädäntöä ei juurikaan ole. CER-direktiivi asettaa selkeitä ja mitattavia vaatimuksia esimerkiksi riskienhallinnan toteuttamistaajuudelle ja tietolähteille.

Nykyinen maailmanpoliittinen turvallisuustilanne ja koronapandemia huomioon ottaen, ovat viisi vuotta sitten valmistunut strategia sekä vuonna 2011 käyttöönotettu valmiuslaki jo osittain vanhentuneet.

Kriittiset toimijat

Suomi on määritellyt huoltovarmuuden kannalta kriittiset toimijat. CER-direktiivissä kuvattu jäsenvaltioiden velvoite tunnistaa nämä toimijat on jo osittain toteutettu. Direktiivistä poiketen Suomen laki huoltovarmuuden turvaamisesta 1390/1992 mukaan kriittisten toimijoiden osallistuminen on vapaaehtoista. Direktiivi esittää kriittisille toimijoille velvoitteita. Velvoitteet voivat olla varsinkin pienemmille toimijoille haaste.

Turvallisuusselvitykset

CER-direktiivin hyväksyminen vaatisi Suomea muuttamaan osin lainsäädäntöään koskien turvallisuusselvityslakia ja lakia henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä tilanteissa, jotka liittyvät suppeisiin turvallisuusselvityksiin EU-rikosrekisteritietojen luovuttamisessa. Kansallista lainsäädäntöä tulisi muuttaa siten, että myös suppeiden turvallisuusselvityksen piiriin kuuluvien henkilöiden osalta voitaisiin hakea tietoja toisen valtion viranomaisten pitämistä rikosrekisteri- tai sakkorekisteritiedoista, koska tällä hetkellä tietojen haku ei ole mahdollista kansallisen lainsäädännön puitteissa. Pääosin kansallinen lainsäädäntö vastaa kuitenkin jo nyt direktiivin vaatimuksia koskien turvallisuusselvityksiä.

Riskien arviointi

Suomen varautuminen määritellään perustuvaksi riskienhallintaan yhteiskunnan turvallisuusstrategiassa. Riskiperusteisuus korostuu myös tiedonhallintalaissa (906/2019, 13 §). Sekä yhteiskunnan turvallisuusstrategiassa että Suomen tietoturvallisuutta ohjaavissa laeissa riskienhallintavaatimukset kuvataan periaatteellisella tasolla, mutta CER-direktiivi tuo riskienhallintaan huomattavan paljon yksityiskohtaisempia vaatimuksia.

CER-direktiivi asettaa riskien arvioinnit tehtäväksi vähintään neljän vuoden välein, joka on ensimmäisen selkeästi mitattava vaatimus riskienhallinnalle. Tämän lisäksi CER-direktiivissä kriittisen toimijan riskienhallinnan täytyy ottaa huomioon sekä Euroopan unionin että yksittäisen jäsenmaan riskiarvio lähtötietoina, joka ohjaa voimakkaasti kriittisen toimijan turvallisuustyötä. Direktiivin mukaan poikkeamailmoitukset tulee jalkauttaa myös riskiarviointeihin jäsenmaatasolla, mikä mahdollistaa kriittiselle toimijalle mittavan aineiston riskiarvion tekemisen tueksi.

Koska kansallisella tasolla Suomessa ei riskienhallintaa ole edellytetty kuin periaatteellisella tasolla, tulee julkishallinnossa todennäköisesti olemaan haasteena yhtenäisen, poikkihallinnollisen riskienhallintamallin luominen ja implementointi niin, että jäsenvaltiotasoinen riskiarvio on jatkettavissa myös edelleen Unionitasolle.

Ilmoitusvelvollisuus

CER-direktiivi asettaa säädöksen piirissä oleville toimijoille velvollisuuden poikkeamien ilmoittamiseen. Ilmoitusvelvollisuudessa vertailukohdaksi voidaan ottaa yleinen tietosuoja-asetus, joskin se on kuitenkin määrityksissään tarkempi. CER-direktiivissä ei suoraan määritellä, kuinka monen tunnin kuluessa huoltovarmuuskriittisen toimijan tulee ilmoittaa siihen kohdistuvasta poikkeamasta, toisin kuin yleisessä tietosuoja-asetuksessa määritellään suoraan tietosuojapoikkeaman ilmoittamisesta valvontaviranomaiselle 72 tunnin kuluessa.

Sanktioinnit

CER-direktiivin seurauksena direktiivin piiriin kuuluvia organisaatioita voidaan rangaista varautumisvelvollisuuden rikkomisesta. CER-direktiivin sanktiointiin liittyvät artiklat on kirjoitettu yhteneväisillä sanamuodoilla Yleisen tietosuoja-asetuksen direktiivien kanssa, joskin CER-direktiivin sanktioinnin vähimmäisvaatimuksia ei ole kuvattu yhtä yksityiskohtaisesti. Varautumiseen liittyvällä sanktioinnilla voi olla sekä positiivisia, että negatiivisia vaikutuksia: Sanktioiden luoma pelote voi parantaa sekä julkishallinnon että yksityisen sektorin varautumista. Toisaalta sanktiot (ja koko CER-direktiivi muine velvoitteineen) voivat vähentää yksityisen sektorin investointihalukkuutta Eurooppaan ja Suomeen.

Lähteet

Euroopan komissio 2020. Euroopan parlamentin ja neuvoston direktiivi kriittisten toimijoiden häiriönsietokyvystä. Viitattu 19.3.2022.
https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52020PC0829

Euroopan Unionin Neuvosto 2009. Neuvoston puitepäätös 2009/315/YOS jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä. Euroopan unionin virallinen lehti L 93/23, Viitattu 18.3.2022. *https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32009F0315*

Huoltovarmuuskeskus 2021. Lausuntopyyntö U 71/2020 vp. Viitattu 19.3.2022.
https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2021-AK-365091.pdf

Iso-Markku, T. 2022. The EU and Finland´s Security of Supply -A 'turn in EU thinking provides new opportunities but significant differences remain. Finnish Institute of International Affairs. Viitattu 15.3.2022.
https://www.fiia.fi/julkaisu/the-eu-and-finlands-security-of-supply

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018. Viitattu 19.3.2022 *https://www.finlex.fi/fi/laki/alkup/2018/20181054*

Laki oikeusrekisterikeskuksesta 625/2012. Viitattu 19.3.2022
https://www.finlex.fi/fi/laki/alkup/2012/20120625#Pidm45237816216144

Luoma, R. 2019. Viranomaisten toimivaltuudet häiriötilanteissa. Oikeusministeriön julkaisuja, Selvityksiä ja ohjeita 2019:18. Viitattu 14.3.2022. *http://urn.fi/URN:ISBN:978-952-259-756-4*

Oikeusministeriö 2021. Säädösvalmistelu OMO38:00/2021: ECRIS-TCN-asetuksen edellyttämää täydentävää lainsäädäntöä ja ECRIS-TCN-direktiivin edellyttämää täytäntöönpanoa koskevaa lainsäädäntöä valmisteleva työryhmä. Viitattu 19.3.2022
https://oikeusministerio.fi/hanke?tunnus=OM038:00/2021

Pelastuslaki 379/2011. Viitattu 13.3.2022. *https://www.finlex.fi/fi/laki/ajantasa/2011/20110379*

Sisäministeriö 2021. Euroopan komission ehdotus Euroopan parlamentin ja neuvoston direktiivin kriittisten toimijoiden häiriönsietokyvystä (Muistio EU/2020/1/1795). Viitattu 14.3.2022
https://www.eduskunta.fi/FI/vaski/Kirjelma/Documents/U_71+2020.pdf

Turvallisuuskomitea 2017. Yhteiskunnan turvallisuusstrategia - Valtioneuvoston periaatepäätös. Viitattu 13.3.2022 *https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2017/*

Turvallisuusselvityslaki 19.9.2014/726. Viitattu 19.3.2022
https://www.finlex.fi/fi/laki/ajantasa/2014/20140726#L3P9

Valmiuslaki 1552/2011. Viitattu 13.3.2022. *https://www.finlex.fi/fi/laki/ajantasa/2011/20111552*

Valtioneuvosto 2022. Periaatepäätökset. Viitattu 19.03.2022
https://valtioneuvosto.fi/paatokset/periaatepaatokset

Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018. Viitattu 19.3.2022.
https://www.finlex.fi/fi/laki/alkup/2018/20181048

10 Toiminnan jatkuvuus ja kyberturvallisuus näkyvillä Laurean opetuksessa ja hanketyössä

Harri Ruoslahti

KYBERTURVALLISUUS ON NOUSSUT yhdeksi Euroopan Unionin strategiseksi turvallisuustavoitteeksi. Kyberuhkiin reagointia voidaan parantaa kyberuhkatietämyksen ja liiketoiminnan jatkuvuuden periaatteiden joustavalla integraatiolla. Laurean turvallisuusalan ja tietojenkäsittelyn opintoja yhdistämällä ja niihin Laurean mukana eurooppalaista kyberresilienssiä rakentavaa hanketyötä integroimalla voidaan tuottaa modernissa tietoyhteiskunnassa tarvittavaa korkealuokkaista liiketoiminnan jatkuvuutta ja kyberuhkatietämystä yhdistävää osaamista.

JOHDANTO

Yhteiskunta ja sen organisaatiot kohtaavat uhkia, jotka useimmiten yllättävät. Vuonna 2020 koronapandemia ja Vastaamon tietomurto olivat näkyviä esimerkkejä toiminnan jatkuvuutta uhkaavista tilanteista. Harva uskoi, että tänä vuonna 2022 Euroopassa käydään Venäjän ja Ukrainan välillä täysmittaista sotaa. Suomen lähestyessä NATO-jäsenyyttä joudumme olettamaan, että suomalaiseenkin yhteiskuntaan saatetaan kohdistaa kyberhäirintää ja hybridiuhkia.

Ennen pandemian puhkeamista kyberhäiriö oli vuoden 2020 Allianz Risk Barometer -kyselyn mukaan ykkösuhka toiminnan jatkuvuudelle. Kyberturvallisuus on myös noussut yhdeksi Euroopan tärkeimmistä strategisista turvallisuustavoitteista. Kyberiskit voivat vaikuttaa monin tavoin jokaisen eurooppalaisen organisaation toimintaan ja ihmisten elämään. Tätä fokusta osoittavat Euroopan komission rahoittamat hank-

keet Cyber Competence Network, Concordia, Cyber Security for Europe, SPARTA ja ECHO. Näiden kaikkien tavoitteina on koota kyberturvallisuuden toimijoita yhteen, vaihtaa tietoa eri alojen välillä ja siten kehittää Euroopalle yhteisempää kyberstrategiaa.

Liiketoiminnan jatkuvuuden lähestymistavan ja kyberuhkatietämyksen joustava integroituminen voi parantaa reagointia ennakoimattomiin kyberuhkiin ja siten osaltaan varmistaa liiketoiminnan jatkuvuuden turvaamista (Rajamäki & Ruoslahti 2022). Kriittisiin infrastruktuureihin kohdistuu enenevässä määrin näiden toiminnan jatkuvuutta uhkaavia kyberuhkia ja siksi nykyisten kompleksisten riippuvuuksien ja vaikutusketjujen arviointiin tarvitaan laajempia menetelmiä, jotka ottavat huomioon resilienssin ja jatkuvuudensuunnittelun vaiheet kyberturvallisuuden prosesseihin ja periaatteisiin (Linkov et al. 2014, 407-408; Pirinen 2017, 265).

Laurea-ammattikorkeakoulun turvallisuusalan opinnot kasvattavat opiskelijoiden valmiuksia ymmärtää ja kohdata organisaatioiden toimintaa uhkaavia riskejä sekä niiden toteutuessa kohdata mahdollisia uhkia ja häiriöitä. Laurealainen opetus perustuu läheiseen yhteystyöhön työelämän kanssa ja siten oppimiseen aidoissa työelämäprojekteissa. Tätä menetelmää kutsutaan nimellä Learning by Delevoping (LbD) ja tämän julkaisun opiskelija-artikkelit ovat eläviä esimerkkejä tästä oppimistavasta.

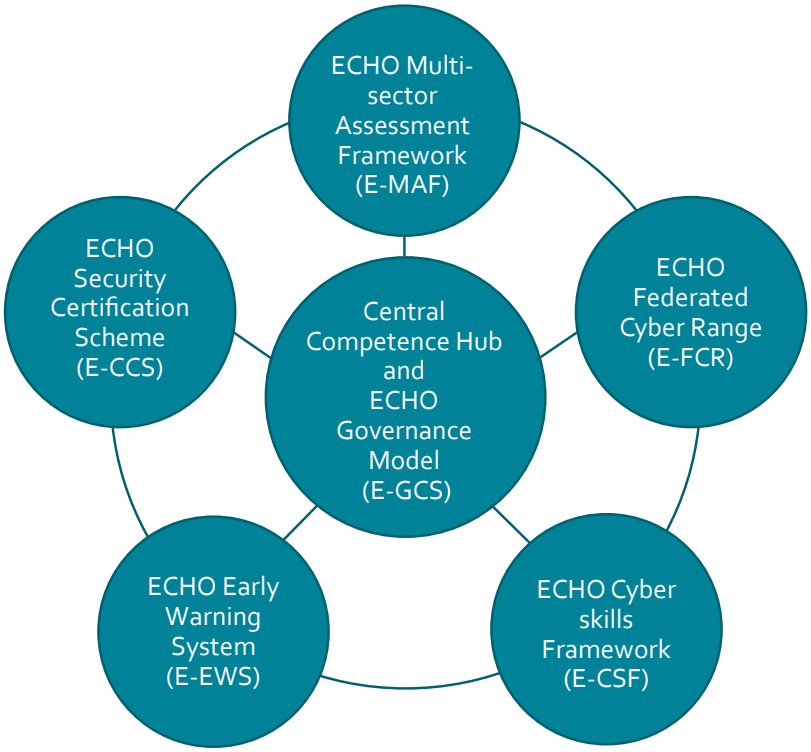
Tämä artikkeli tarkastelee turvallisuusalan opintoja Laureassa sekä sitä, miten opinnot ja Laurean hanketoiminta kytkeytyvät yhteen ja tuottavat ulkoisen rahoituksen lisäksi mahdollisuuksia oppimiseen sekä julkaisuihin. Artikkelissa esitellään tarkemmin kaksi Euroopan komission rahoittamaa liiketoiminnan jatkuvuuteen ja kyberturvallisuuteen liittyvää hanketta (ECHO ja DYNAMO), jotka tarjoavat opiskelijoille mahdollisuuksia oppimiseen eurooppalaisen tutkimus- ja innovaatiotyön parissa.

LAUREA JA EUROOPAN KYBERRESILIENSSI

Pöyhönen ym. (2020) korostaa, että kyberturvallisuus tavoittelee ajantasaiseen tilanneymmärrykseen perustuvia resilienttejä järjestelmiä ja infrastruktuuria. Yhteiskunnan toiminnan kannalta on erityisen tärkeää, että kriittisen infrastruktuurin toiminnot kyetään säilyttämään (Ruoslahti 2020a).

Laurea kuuluu vuosina 2019–2023 toteutettavan ECHO-hankkeen (the European network of Cybersecurity centres and competence Hub for innovation and Operations) konsortioon. ECHO-hanke osaltaan vahvistaa Euroopan Unionin proaktiivista kyberpuolustusta ja edistää Euroopan teknologista itsenäisyyttä tehokkaan ja toimivan monialaisen yhteistyön keinoin. Hanke siten osaltaan kehittää eurooppalaista ekosysteemiä, tukee turvallisuusalan yhteistyötä ja kehittää yhtenäistä Euroopan kyberturvallisuusmarkkinaa paremmin suojelemaan EU:n kansalaisia kyberuhilta.

ECHO-hankkeen luoman verkoston tarkoitus on laajentua ja jäädä hankkeen päätyttyä aktiiviseen toimintaan. Yhtenäinen ECHO-hallintomalli (Governance Model) suuntaa verkoston toimintaa ja verkostokumppaneiden osallisuutta sekä hallinnoi kehitettäviä ECHO-palveluita (Kuvio 1).



Kuvio 1. *ECHO-palvelut. Kuvio: www.echonetwork.eu, muokattu.*

Riskienarvioinnin ja -hallinnan työkalu (ECHO Multi-sector assessment framework) huomioi sekä alakohtaisia että monialaisia tarpeita ja uhkia, joiden pohjalta voidaan riskipohjaisesti tunnistaa teknologian ja tuotekehityksen tarpeita ja suuntaa. ECHO Early Warning System (E-EWS), uhkien varhaisen havaitsemisen varoitusjärjestelmä tarjoaa mahdollisuuden jakaa tietoa kyberuhista, -tapahtumista ja trendeistä turvatusti yhteistyössä luotettujen kumppaneiden kesken. ECHO Federated Cyber Range (E-FCR) kybersimulaation, harjoittelun ja tuotekehityksen tueksi hanke edistää simulaatioympäristöjen yhteistoimintaa kokoamalla niitä yhteen simulointiympäristöpalveluun. Tämä mahdollistaa laajojen kokonaisuuksien simuloinnin ja yhteistyön realistisissa oppimis- ja harjoitusympäristöissä. Näiden kahden palvelun lisäksi kybertaitojen kehittäminen nähdään hankkeessa olennaisena osana kyberturvallisuuden parantamisessa kuten myös eurooppalaisten sertifiointijärjestelmien edelleen kehittäminen.

ECHO-palveluiden testaus ja validointi mahdollistavat monialaisten haasteiden ja mahdollisuuksien edelleen tunnistamisen tulevan kehitystyön ja teknologiavalintojen pohjaksi. Hankkeen voidaan nähdä vaikuttavan valtiotason kyberturvallisuuteen tarjoamillaan innovatiivisilla ratkaisuillaan sekä edistämällä mm. kyberturvallisuuskeskusten välistä tiedonvaihtoa ja yhteistyötä kyberuhkien havaitsemiseksi ja torjumiseksi sekä niiden vaikutusten minimoimiseksi. Organisaatiotasolla hanke edistää tietoisuutta siitä miksi ja miten suojata itsensä, asiakkaansa ja verkostonsa ja siten säilyttää maine ja markkina-asema.

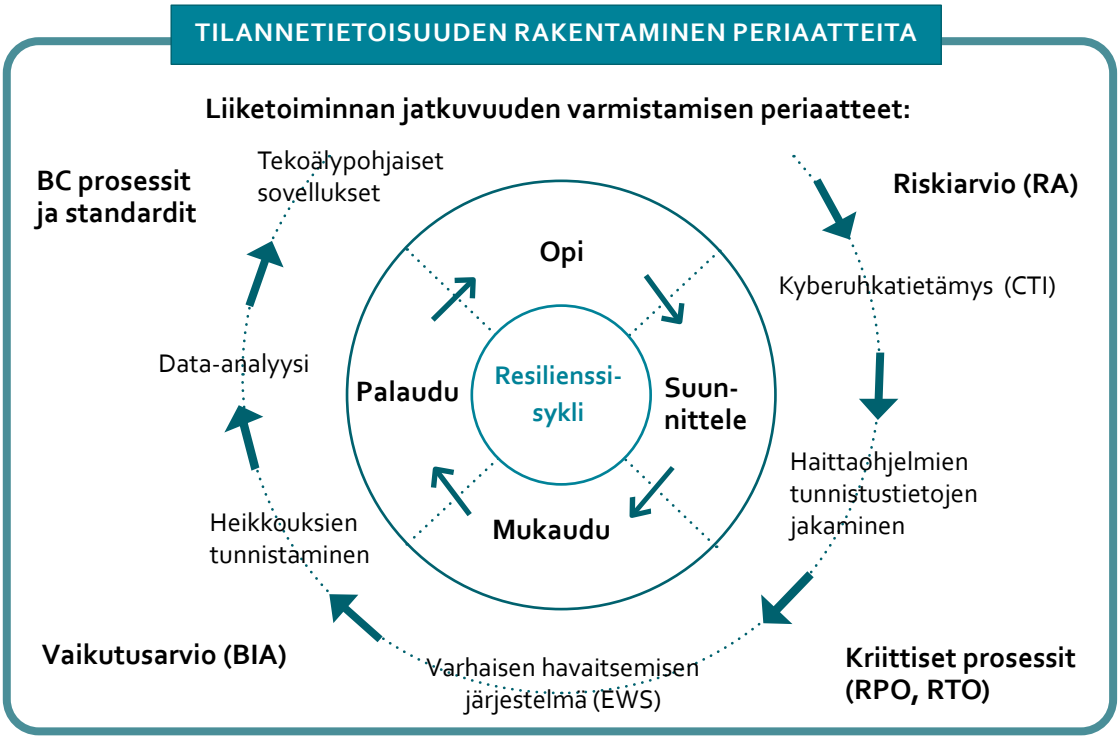
Business Continuity Management + Cyber Threat Intelligence = DYNAMO

Toiminnan muutosten ymmärtäminen resilienssin eri vaiheissa, suunnittele, mukaudu, palaudu ja opi / muutu, edesauttaa nopeaa havaitsemista ja asianmukaista vastetta tuomaan tasapainoa ja kestävyyttä. *"Kun eri alojen ammattilaiset työskentelevät yhdessä loppukäyttäjien kanssa, voidaan loppukäyttäjien tarpeisiin, inhimillisiin tekijöihin, korkeisiin eettisiin standardeihin ja yhteiskunnallisiin vaikutuksiin parhaiten mukautua"* (Rajamäki & Ruoslahti, 2022, 17).

DYNAMO-hankkeen tarkoituksena on vuosina 2022–2025 tuottaa yhteistä pohjaa ja prosesseja tukevaa teknologiaa eri sektoreille tehtäville riskien ja niiden vaikuttavuuden arvioinnille. Hanke toimii loogisena jatkeena sekä Laurean ECHO-hankkeessa tehdylle työlle, että koulussa annettavalle tutkintokoulutukselle. Tänä vuonna EU komissiolta rahoituksen saanut DYNAMO yhdistää periaatteita kahdelta eri osa-alueelta: Business Continuity Management (BCM) eli liiketoiminnan jatkuvuuden turvaaminen sekä Cyber Threat Intelligence (CTI) kyberuhkatietämys perustuen erilaisista lähteistä saatuun analysoituun informaatioon. BCM ja CTI -periaatteiden yhdistäminen tuottaa joustavampia mahdollisuuksia tuottaa päätöksenteon pohjaksi tarvittavaa laajaa ja tarkkaa ajankohtaista kybertilannekuvaa resilienssisyklin kaikissa vaiheissa.

DYNAMO-hankesuunnitelman mukaan ajankohtaiset resilienssiarviot voivat toimia toiminnan jatkuvuuden hallinnan (BCM) pohjana. Yksityiskohtaistakin tietoa sisältävä arvio tarjoaa selkeän arvion tarkasteltavana olevasta sektorista ja sen kriittisistä prosesseista. Loppukäyttäjädata yhdistettynä toimintokuvauksiin ja suoritustavoitteisiin sekä tekoälysovelluksiin auttavat ymmärtämään yhteisten prosessien ja itseoppimisen arvon. Tuloksena on mm. tietoa tarkasteltavan sektorin haavoittuvuuksista suhteessa resilienssin vaiheisiin.

CTI-ratkaisuja jotka lisäävät tietämystä kyberuhista voidaan rakentaa olemassa oleville ratkaisuille kuten ECHO Early Warning System (EWS) jota DYNAMO-hanke kehittää edelleen. Haittaohjelmien tunnistustiedon jakaminen voidaan tehdä yhteisellä EWS:n kanssa integroidulla Malware Information Sharing Platform (MISP) - alustalla nostamaan tilannetietoisuuttaa eri sektoreiden turvallisuustoimijoiden kesken. Nämä ratkaisut integroidaan resilienssin periaatteita hyödyntäen, BCM-prosesseja noudattaen ja tekoälyn mahdollisuuksia käyttäen (Kuvio 2).



Kuvio 2. *DYNAMO tilannetietoisuus kyberresilienssin rakentajana (muokattu DYNAMO).*

Suuri haaste on luoda vakaa ja tehokas valtioiden, organisaatioiden ja yritysten välinen yhteistyöverkosto kyberturvallisuuteen liittyvien tiedon, taitojen ja resurssien jakamiseen EU:n alueella. Tietoa jakamalla voidaan lisätä tietoisuutta kyberturvallisuuden tärkeydestä ja keinoista ja siten saavuttaa Euroopan laajuisesti parempaa yhteistä ymmärrystä kyberuhista sekä niiden torjunnasta sekä jakaa parhaita kokemuksia kyberriskien hallinnasta ja käsittelystä.

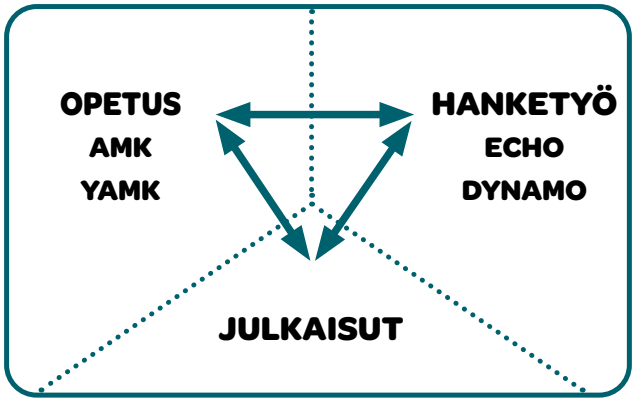
LBD – LAUREASSA TYÖ TEKIJÄÄNSÄ OPETTAA

Laurealainen asiantuntijuus näkyy ja kasvaa hanketyötä tehtäessä. Tämä koskee sekä hankkeisiin tutkijoina ja asiantuntijoina osallistuvia opettajia, että niistä opintopisteitä kerääviä opiskelijoita. Laurea osallistuu ECHO- ja DYNAMO-hankkeissa moniin eri työpaketteihin. ECHO:ssa Laurea mm. vastaa yhteiskunnallisten vaikutusten arviointityökalujen kehittämisesti ja pilotoinnista. Asianmukaisten teknologioiden, tuotteiden ja palveluiden lisäksi kyberturvallisuuteen vaikutetaan kehittämällä ihmisten tietoisuutta ja taitoja tunnistaa kyberuhkia sekä tarvittaessa torjua niitä. ECHO:ssa kehitettyä yhteiskunnallisia vaikutuksia luotavaa kyselytyökalua sovelletaan myös DYNAMO:ssa millä saavutetaan EU:n toivomaa ja Laureaa hyödyttävää jatkuvuutta.

Toinen Laurean tekemä työ ECHO-hankkeessa tutkii organisaatiokohtaisia e-taitoja. ECHO:n rahoituksella on kehitetty e-taitojen puuteanalyysityökalu, joka vertaa toivottua tavoitetasoa henkilökohtaisten itse- ja 360-vertaisarvioiden kautta kerättyyn vallitsevaan taitotilanteeseen. Tätä työkalua pilotoidaan ECHO-hankkeessa sekä hyödynnetään ja kehitetään edelleen osana DYNAMO:a. Näillä kahdella työkalulla tehdyistä tapaustutkimuksista julkaistaan akateemisia artikkeleita, jotka voidaan liittää osaksi hankkeen tuotoksia. Näin hanketyö mahdollistaa opettajille ja opiskelijoille mahdollisuuksia laajentaa omaa ja laurealaista tietämystä ja hankkeen tietoperustaa kirjoittamalla opinnäytetöitä ja tieteellisiä artikkeleita. Tällainen työskentelytapa lisää hankkeessa tuotettujen julkaisujen määrää, joita voidaan käyttää lähteinä, kun tuotetaan EU komissiolle luvattuja virallisia hankeraportteja.

Laurean järjestämät tapahtumat kuten esimerkiksi kaikille avoin Laurea Cyber Morning, osaltaan helpottaa kyberturvallisuuteen kytkeytyvän hanketyön integroimista Laurean turvallisuusalan ja tietojenkäsittelyn koulutusohjelmiin sekä osaltaan lisää Laurean vaikuttavuutta myös laajemmalle yleisölle.

Learning by Developing periaatteen mukaisesti tämän kaltaiset hankkeet ovat siis oivia oppimisympäristöjä Laurean opiskelijoille – ja opettajille. Laureassa kehitetty LbD toimintamalli mahdollistaa korkeakoulun opetustehtävän integroinnin palvelemaan tutkimusta (Rajamäki, 2021). Esimerkiksi ECHO-hanke mahdollistaa opintopisteiden ansaitsemisen kaikilla mahdollisilla tavoilla, hanke integroituu opintojaksoille ja tarjoaa mahdollisuuksia soveltaa ja laajentaa hankeen tietoperustaa projektipisteinä, harjoitteluna ja opinnäytetöinä (Kuvio 3).



Kuvio 3. *Opetus-hanketyö-julkaisut–sykli. Kuvio: Harri Ruoslahti.*

Kuvio 3 osoittaa, miten hankkeisiin kirjoitettujen julkaisujen tuottamaa tietoa voidaan soveltaa hanketyön lisäksi oppimisessa ja opetuksessa. Julkaisut osaltaan edistävät kirjoittajien osaamisen kehittymistä ja laajentavat Laurean vaikuttavuutta. Konferensseissa esitetty työ saattaa mahdollistaa suoran vuorovaikutuksen alan ehdottomien huippujen kanssa. On tärkeää, että laurealaisille tutkijoille tarjotaan mahdollisuuksia julkaista työtään ja verkostoitua samoista aiheista kiinnostuneiden muiden turvallisuusalan tutkijoiden kanssa.

JATKUVUUDEN HALLINTA LAUREAN TURVALLISUUSALAN OPINTOJEN YTIMESSÄ

Rajamäki ja Ruoslahti (2018) ehdottavat korkeakouluopetukseen malleja, joiden avulla opiskelijat voisivat työelämässä ylläpitää organisaationsa kriittisiä toimintoja ja rakentaa resilienttiä liiketoiminnan jatkuvuutta. Laureassa jatkuvuuden opinnot pyrkivät valmentamaan Laureasta valmistuvia asiantuntijoita ymmärtämään yhteiskuntaa ja sen organisaatioita (yrityksiä ja julkishallintoa) sekä suunnittelemaan ja tarvittaessa kohtaamaan toimintaa uhkaavia äkillisiä odottamattomia tapahtumia.

Riskien arviointi ja jatkuvuuden hallinta ovat keskiössä kolmessa Laurean tutkinnossa, suomenkielisessä Turvallisuus ja riskienhallinta sekä englanninkielisessä Safety, security and risk management (AMK) sekä Turvallisuusjohtaminen (YAMK). Näin Laurean turvallisuusalalta valmistuneet ymmärtävät huolellisen suunnittelun, tilanteen mukaisen reagoinnin ja kokemuksista oppimisen roolin kriittisten toimintojen ylläpitämiseksi vaikeinakin hetkinä. Laureasta valmistuneet osaavat soveltaa riskien ja vaikutusten analyysityökaluja sekä alan keskeisiä prosesseja ja standardeja. Kyberturvallisuuteen voi perehtyä Laurean tietojenkäsittelyn opinnoissa.

Tämän julkaisun opiskelijakirjoittajat opiskelevat YAMK-tutkintoa Turvallisuusjohtaminen. Opinnoissa keskitytään valmiuksiin turvallisuuden eri osa-alueilla: turvallisuuden johtaminen riskienhallintaprosessissa, yksilön ja organisaation turvallisuuskäyttäytyminen, strateginen johtaminen, turvallisuuden johtaminen yrityksen kansainvälisessä toiminnassa, kyberturvallisuus sekä toiminnan jatkuvuuden varmistaminen. Artikkelit on kirjoitettu osana Toiminnan jatkuvuuden varmistaminen -opintojaksoa.

Kriiseihin valmistautuminen on kollektiivinen prosessi, jossa toimijat valmistautuvat kohtaamaan häiriöitä yhdessä. Näin he, yhteisiin kokemuksiinsa perustuen, oppivat ja sopeutumaan mahdollisiin kyberhäiriöihin. Monet sosiaaliset verkostot ovat kuitenkin toiminnoiltaan varsin kompleksia ja resilienssin näkökulmasta turbulenteissa toimintaympäristöissä tarvitaan joustavuutta. Näin voidaan työskennellä kohti parempaa yhteistoiminnan resilienssiä (Ruoslahti 2020b).

Lähteet

Linkov, I., Bridges, T., Creutzig, F., Decker, J. Fox-Lent, C., Kröger, W., Lambert, J.H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. 2014. Changing the resilience paradigm, Nature Climate Change, 4 (6), 407–409.

Pirinen, R. 2017. Towards Common Information Systems Maturity Validation - Resilience Readiness Levels (ResRL). Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 3: ISE, 259–266.

Pöyhönen, J., Rajamäki, J., Lehto, M. & Ruoslahti, H. 2020. Cyber Situational Awareness in Critical Infrastructure Protection. Annals of Disaster Risk Sciences, 3 (1): Special issue on cyber-security of critical infrastructure. *https://ojs.vvg.hr/index.php/adrs*

Rajamäki, J. 2021. Aktiivista osallistumista huippututkimukseen sekä oppimista EU:n puiteohjelmahankkeissa – ECHO. Teoksessa Kallunki, V., Lumia, M., Pahkin, K., Seppänen, S., Ylikoski,T. & Merimaa, M. (toim.) Askel askeleelta kohti strategista muutosta Laureassa. Vantaa: Laurea-ammattikorkeakoulu, 178-181. *https://urn.fi/URN:ISBN:978-951-799-628-0*

Rajamäki, J. & Ruoslahti, H. 2022. Organisaation ennakointikyvykkyyden johtaminen muuttuvissa kybertoimintaympäristöissä resilienssiajattelulla. 3UAS: Tulevaisuudenkestävä bisnes – osaaminen systeemeissä: Johtaminen tulevaisuuden toimintaympäristössä / Paperi 51 / Track 3: Muutokset tulevaisuuden toimintaympäristöissä ja tulevaisuuslukutaito, verkossa 27.4.2022.

Ruoslahti, H. 2020a. Business Continuity for Critical Infrastructure Operators. Annals of Disaster Risk Sciences, 3 (1): Special issue on cyber-security of critical infrastructure. *https://ojs.vvg.hr/index.php/adrs*

Ruoslahti, H. 2020b. Yhteiskehittäminen EU-rahoitetuissa hankkeissa. Tiede ja ase, Sotatieteellisen seuran vuosijulkaisu n:o 78. Helsinki: Suomen sotatieteellinen seura.

LAUREA

AMMATTIKORKEAKOULU

University of Applied Sciences

Tämän julkaisun *Jatkuvuutta turvaamassa – Laurea YAMK opiskelijoiden näkökulmia* artikkelit ovat kirjoittaneet Laurea YAMK Turvallisuusjohtamisen opintojakson Toiminnan jatkuvuuden varmistaminen opiskelijat ja opettajat.

Opiskelijoiden artikkelit on toteutettu yhteiskehittämisenä. Ensimmäisessä vaiheessa kukin opiskelija etsi henkilökohtaisena tehtävinä neljä jatkuvuuden hallintaa käsittelevää akateemista artikkelia tai raporttia. Nämä koottiin kaikille avoimeksi yhteiskäyttöiseksi lähdekirjallisuuslistaksi. Jokainen Opiskelija myös haastatteli yhteistä haastattelupohjaa käyttäen toiminnan jatkuvuuden asiantuntijaa.

Jakauduttuaan tiimeihin opiskelijat hyödynsivät löytämiään lähteitä ja käymiään haastatteluita ja valitsivat tiiminsä artikkelille näkökulman. Näiltä pohjilta opiskelijat ovat tiimeinä yhteiskirjoittaneet tähän julkaisuun tulleet artikkelit.