SAVONIA

MUU RAPORTTI - **YLEMPI AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

ORGANISAATION KYBER-TURVALLISUUSKYVYKKYY-DEN KEHITTÄMINEN

TEKIJÄ: Kimmo Väisänen EJJ19SY

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Teknologiaosaamisen johtamisen tutkinto-ohjelma	
Työn tekijä(t) Kimmo Väisänen	
Työn nimi Organisaation kyberturvallisuuskyvykkyyden kehittäminen	
Päiväys 18.4.2022	Sivumäärä/Liitteet 65/30
Toimeksiantaja/Yhteistyökumppani(t) AddSecure Oy	

Tiivistelmä

Opinnäytetyön tavoitteena oli selvittää, millainen kyberturvallisuuden hallintamalli organisaatiolla tulee olla, jotta se täyttää kriittisten viranomaisasiakkaiden perustason tietosuojavaatimukset. Mikäli luottamuksellisen tiedon suojaamistoimenpiteet tehdään puutteellisesti tai tarpeettoman laajasti, vaarantaa se joko salassa pidettävän tiedon luottamuksellisuuden tai aiheuttaa organisaatiolle ylimääräisiä kustannuksia liian laajasti ja vaikeasti ylläpidettävien suojaamistoimenpiteiden takia.

Opinnäytetyö toteutettiin tapaustutkimuksena. Kyberturvallisuuteen vaikuttavat asiat haluttiin ymmärtää syvällisesti, jotta sen kehittämiseen voidaan tehdä kehittämisehdotuksia. Opinnäytetyössä hyödynnettiin myös toimintatutkimuksen kvalitatiivisia eli laadullisia menetelmiä, koska organisaation kyberturvallisuuskyvykkyyden nykytilan arviointiin osallistui organisaation työntekijöitä. Samalla heidän kybertietoisuutensa kasvoi ja toiveena oli, että he alkaisivat tämän selvityksen myötä pohtia myös omaan työtehtäväänsä kyberturvallisuuden näkökulmasta.

Opinnäytetyön teoriaosuudessa tutustuttiin laajasti kyberturvallisuutta koskeviin kotimaisiin ja ulkomaisiin lähteisiin. Näiden pohjalta summattiin yhteen ne keskeiset kyberturvallisuuden hallintaan vaikuttavat tekijät, jotka organisaation tulee toiminnassaan huomioida. Työssä kartoitettiin myös NIST Framework Core-viitekehyksen pohjalta erilaisia kyberturvallisuuden hallintakeinoja, joita toteuttamalla organisaatio pystyy kehittää omaa kyberturvallisuuskyvykkyyttään kyberhäiriötilanteiden tunnistamisen, suojautumisen, havaitsemisen, reagoimisen sekä palautumisen osalta.

Opinnäytetyön tutkimuksellisen osuuden tavoitteena oli tunnistaa puutteet, joita organisaation tulee kehittää asetettuihin kyberturvallisuustavoitteisiinsa pääsemiseksi. Kohdeorganisaatiolle suoritettiin sisäinen kyberturvallisuuskypsyyden nykytila-analyysi Kyberturvallisuuskeskuksen Kybermittarin avulla. Analyysin tueksi toteutettiin myös Katakri 2020-auditointityökalulla itsearviointi viranomaisten salassa pidettävien tietoaineistojen käsittelykyvystä. Näiden kahden arvioinnin pohjalta organisaatiolle laadittiin suunnitelma myöhemmin toteutettaville kehitystoimenpiteille.

Opinnäytetyön lopputuloksena organisaatiolle syntyi hyvä käsitys kyberturvallisuuden hallintaan vaikuttavista tekijöistä ja selkeä toimenpidelista asioista, jotka suorittamalla pääsemme tavoitellulle kypsyystasolle kyberturvallisuuskypsyyden kehittämisen portaikossa. Hyvä oppi oli myös ymmärtää, kuinka moni eri asia vaikuttaa organisaation kyberturvallisuuskyvykkyyteen, kuin myös se, että kyberturvallisuuskyvykkyyden kehittäminen on jatkuva prosessi, joka ei koskaan tule täysin valmiiksi.

Avainsanat

Kyberturvallisuus, haavoittuvuus, riskienhallinta, varautuminen, jatkuvuudenhallinta, kybermittari

SAVONIA UNIVERSITY OF APPLIED SCIENCES THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Master's Degree Programme in Engineering Knowledge Management	
Author(s) Kimmo Väisänen	
Title of Thesis Developing an organization's cybersecurity capabilities	
Date 18.4.2022	Pages/Appendices 65/30
Client Organisation /Partners AddSecure Oy	

Abstract

The aim of the thesis was to find out what kind of cyber security management model an organization should have to meet the basic data protection requirements of critical authority customers. Inadequate or unnecessarily extensive protection measures for confidential information will compromise the confidentiality of confidential information or impose additional costs on the organization due to protection measures that are too oversized and difficult to maintain.

The thesis project was carried out as a case study. There was a deep desire to understand the issues contributing to cyber security in order to generate development suggestions for its development. The thesis also utilized the qualitative methods of action research, because the employees of the organization participated in the evaluation of the current state of the organization's cyber security capabilities. Simultaneously, their cyber awareness increased, and it was hoped that with this evaluation they would also start to consider their own work from the perspective of cyber security.

Firstly, in the theoretical part of the thesis, domestic and international sources concerning cyber security were extensively studied. Secondly, based on these, the key factors influencing cyber security management that the organization must consider in its operations were summed up. Based on the NIST Framework Core, the work also mapped out various cybersecurity management tools that enable an organization to develop its own cybersecurity capabilities for identifying, protecting, detecting, responding to, and recovering from cyber incidents.

The aim of the research part of the thesis was to identify the shortcomings that an organization must develop to achieve its set cyber security goals. An internal analysis of the current state of cyber security maturity was performed for the target organization using the Cybermeter from the Cyber Security Center. To support the analysis, the Katakri 2020 audit tool was also utilised to conduct a self-assessment of the authorities' ability to process confidential data. Finally, based on these two evaluations, a plan was developed for the organization for future development measures.

In conclusion, as a result of the thesis, the organization gained a good understanding of the factors influencing cyber security management and a clear list of measures that, when completed, will reach the desired level of maturity at the stage of developing cyber security maturity. It was also beneficial to understand how many different factors affect an organization's cybersecurity capabilities, as well as the fact that developing cybersecurity capabilities is an ongoing process that will never be fully completed.

Keywords
Cyber security, Vulnerability, Risk management, Preparedness, Continuity management, Cybermeter

ESIPUHE

Haluan kiittää AddSecure Oy:tä mielenkiintoisesta opinnäytetyön aiheesta. Aihe on hyvin ajankohtainen maailman nopeasti muuttuneessa turvallisuustilanteessa ja oli motivoivaa tutkia aihetta, joka auttaa jatkossa entistä selkeämmin kehittämään oman työyhteisön kyberturvallisuuden hallintaa.

Kiitokset haluan antaa myös opinnäytetyötä ohjanneille yliopettaja Veli-Matti Tolpille sekä AddSecuren Offering Managerille Jari Kentälle, jotka antoivat hyviä näkökulmia, miten aiheita opinnäytetyössä kannattaa käsitellä.

Lopuksi tahdon kiittää myös perhettäni tuesta ja kannustuksesta opinnäytetyön aikana.

Kuopiossa 18.4.2022
Kimmo Väisänen

SISÄLTÖ

LYHENTEET JA MÄÄRITELMÄT 7
1 JOHDANTO 9
1.1 Toimeksiantaja ja työn taustaa 10
1.2 Työn rakenne 10
1.3 Viitekehys, tavoitteet, tutkimusongelma ja aiheen rajaus 12
1.4 Tutkimusote ja metodologia 13
1.5 Työn etenemisen vaiheet ja aikataulu 14
2 KYBERTURVALLISUUS 16
2.1 Kyberturvallisuus on osa digitaalisen turvallisuuden viitekehystä 16
2.2 Organisaatioon kohdistuvia kyberuhkia 17
2.2.1 Tietojenkalastelu 18
2.2.2 Haittaohjelmat 18
2.2.3 Kiristysohjelmat 18
2.2.4 Palveluestohyökkäykset 19
2.3 Haittaohjelmahyökkäyksen kohteeksi joutumisen syitä 19
2.4 Haittaohjelmahyökkäyksen toteutus 20
2.5 Kyberhäiriön vakavuus 21
2.6 Kyberturvallisuuden nykytila Suomessa ja maailmalla 22
3 LAINSÄÄDÄNTÖ- JA VIRANOMAISVAATIMUKSET 26
3.1 Lainsäädäntöön ja asiakassopimuksiin perustuvat vaatimukset 26
3.2 Tietoaineiston käsittely ja luokittelu 27
3.3 Tiedon suojaaminen 28
3.4 Tietoturvallisuuden perustason vaatimukset 29
3.5 Toimittajien jatkuvuudenhallinta vaatimukset 30
4 KYBERTURVALLISUUDEN HALLINTA JA KEHITTÄMINEN 31
4.1 Toiminnan jatkuvuuden hallinta 31
4.2 Varautuminen on ennakointia 32
4.3 Riskienhallintaprosessi 32
4.3.1 Riskien tunnistaminen ja arviointi 33
4.3.2 Riskien hallintakeinot 33

4.3.3 Riskien seuranta ja vahingosta oppiminen 34
4.4 Kyberturvallisuus tarvitsee johtamista 35
4.5 Kyberturvallisuuden johtamis- ja hallintamalli 35
4.6 NIST-kyberturvallisuuden viitekehys 37
4.6.1 Viitekehyksen rakenne 38
4.6.2 Kyberturvallisuusympäristön ja riskien tunnistaminen (Identify) 39
4.6.3 Kyberhäiriötilanteilta suojautuminen (Protect) 40
4.6.4 Kyberhäiriötilanteen havaitseminen (Detect) 41
4.6.5 Kyberhäiriötilanteeseen reagointi (Respond) 41
4.6.6 Kyberhäiriötilanteesta palautuminen (Recover) 42
4.7 Työkaluja hallintamallin kehittämiseen 42
4.7.1 ISO/IEC 27000 -standardi 43
4.7.2 Katakri 2020 43
4.7.3 Vahti -ohjeet 44
4.8 Hallintamallin kehittäminen on evoluutioprosessi 45
5 KYBERTURVALLISUUDEN MITTAAMINEN 47
5.1 Kyberturvallisuuden vuositavoitteet 47
5.2 Arviointi- ja mittausmenetelmät 47
5.3 Kyberturvallisuuden mittaristo ja sen kehittäminen 49
5.4 Traficomin Kybermittari 51
5.5 Kyberturvallisuuskyvykkyyden perustason vaatimukset 52
6 TYÖN TULOKSET JA JOHTOPÄÄTÖKSET 54
6.1 Tärkeimmät tulokset ja johtopäätökset 54
6.2 Onnistumiset ja haasteet 56
6.3 Jatkokehitystarpeet 56
6.4 Jatkotutkimusaihe 57
7 YHTEENVETO 58
LÄHTEET 59
LIITE 1 KYBERTURVALLISUUDEN NYKYTILA-ANALYYSI 63
LIITE 2 TULOSTEN ARVIOINTI 64
LIITE 3 KEHITYSEHDOTUKSET 65

LYHENTEET JA MÄÄRITELMÄT

Digitaalinen turvallisuus	Kyberturvallisuuden synonyymi ja se pitää sisällään toimenpiteitä liittyen organisaation riskienhallintaan, jatkuvuudenhallintaan, varautumiseen, tietoturvallisuuteen sekä tietosuojaan.
Eheys	Sähköinen tieto ei saa muuttua hallitsemattomasti.
Haavoittuvuus	Sähköiseen tiedonsiirtoon liittyvä heikkous, joka mahdollistaa vahingon toteutumisen tai sitä voidaan hyödyntää vahingon aiheuttamisessa.
Jatkuvuudenhallinta	Toimintaprosessi, jolla tunnistetaan organisaatiota uhkaavia tekijöitä, arvioidaan uhkien vaikutukset ja määritetään häiriötilanteita varten hallintakeinoja toiminnan jatkuvuuden varmistamiseksi.
Kohdistettu hyökkäys	Tietoturvaloukkaus, joka on kohdistettu tiettyyn toimijaan. Haittaohjelman asennuksessa hyödynnetään tunnettuja ohjelmistohaavoittuvuuksia.
Kybermittari	Kyberturvallisuuskeskuksen kehittämä mittari, jolla organisaatio voi arvioida omaa kyberturvallisuuden kypsyystasoa.
Kyberturvallisuus	Tavoitetila, jossa organisaation kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvata.
Kyberturvallisuusarkkitehtuuri	Kyberturvallisuusarkkitehtuuri on olennainen osa yrityksen tietojärjestelmien kokonaisarkkitehtuuria. Sen avulla kuvataan organisaation turvallisuusprosessien, kyberturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin.
Kyberturvallisuusstrategia	Yrityksen kyberturvallisuusstrategia on kyberturvallisuuden kehityksen perusta. Yksinkertaisimmillaan yrityksen kyberturvallisuusstrategiassa on kyberturvallisuuden tavoitteet ja suunnitelma niiden saavuttamiseksi.
Luottamuksellisuus	Luokiteltua tai salassa pidettävää tietoa voivat saada käyttöönsä vain tahot, jolla on käyttöoikeus siihen.
NIST (National Institute of Standards and Technology)	NIST on yhdysvaltalainen kauppaministeriön virasto, joka laatii kyberturvallisuutta ja yksityisyyden suojaan määritteleviä standardeja sekä parhaita käytäntöjä, joilla autetaan organisaatiota hallitsemaan kyberturvallisuutta.

Riskienhallinta	Toimintaprosessi, joka kattaa riskianalyysin sekä riskienhallinnassa tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet.
Saatavuus	Tietojen tulee olla saatavilla niitä tarvitseville käyttäjille palvelussa edellytettävällä vasteajalla (SLA).
Tietoaineisto, tieto (data)	Suojattava asia, tässä tapauksessa sähköisessä muodossa oleva tieto.
Tietosuoja	Henkilön yksityisyyden ja häntä koskevien tietojen suojaaminen oikeudettomalta käytöltä henkilötietoja käsiteltäessä
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista.
Tietoturvapoikkeama	Haitallinen tietoturvaan liittyvä tapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvallisuuden ja voi vaikuttaa organisaation toimintaan negatiivisesti.
Varautuminen	Prosessi, jolla varmistetaan organisaation mahdollisimman häiriötön toiminta sekä tarvittavat toimenpiteet häiriötilanteissa.

1 JOHDANTO

Elämme kyberturvallisuuden keskellä – halusimmepa sitä tai emme. Uutiset tuovat päivittäin tietoomme kyberturvallisuutta yrityksiin kohdistuneiden tietomurtojen ja kybervakoilun muodossa. Henkilökohtaisella tasolla emme juuri kiinnitä huomiota siihen, miten riippuvaisia olemme digitaalisesta maailmasta. Ilman toimivaa tietoliikenneyhteyttä uutiset ja sähköpostit jäisivät aamulla älypuhelimesta tarkistamatta ja auto huoltoasemalla tankkaamatta tai ostokset kaupassa tekemättä. Digitalisoitumista tapahtuu kaikkialla ja luotamme vahvasti kybermaailman toimivuuteen ja sen turvallisuuteen. Vieläkin on organisaatioita ja henkilöitä, jotka ajattelevat, ettei kyberturvallisuus kosketa heitä. (Väestörekisterikeskus 2019, 17). Cyberintin mukaan 43 % kyberhyökkäyksistä kohdistuu kuitenkin pieniin yrityksiin. (Cybinsolutions 2022, Artikkeli). Kyberrikollisten huijausviestit lähtevät kuitenkin päivittäin lukemattomiin sattumanvaraisiin nettiosoitteisiin ja automaattiset skannausohjelmistot etsivät netistä jatkuvasti tietoturva-aukkoja kuten palvelimia, joiden ohjelmistoja ei ole päivitetty ajan tasalle. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen mukaan kyberrikollisuus on globaalia ja automatisoitua toimintaa ja tästä syystä huijausten ja tietomurtojen kohteeksi voi joutua mikä tahansa organisaatio tai toimiala. (Huoltovarmuuskeskus 2021, Artikkeli) Kyberrikollisuuden määrä on kasvanut COVID-19 pandemian aikana yli 600 %. Syynä tähän on se, että yhä useampi kyberrikollinen hyödyntää tilaisuutta esiintyä terveydenhuollon toimijana ja saa sitä kautta vastaanottajat klikkaamaan epäilyttäviä linkkejä tai lataamaan haitallisia ohjelmia. (Purplesec 2021, Artikkeli).

Mitä tietoisia toimenpiteitä voisimme tehdä organisaation kyberturvallisuuskyvykkyyden kehittämiseksi? Organisaation näkökulmasta kyberturvallisuuden pitäisi olla strateginen valinta. Lähes kaikki organisaatiot käsittelevät jollakin tasolla toisen organisaation luottamuksellista tietoa. Asiakastiedon suojaaminen on kriittinen menestystekijä palvelua tuottavan organisaation toiminnalle ja kehittymiselle ja uusien liiketoimintamallien toteuttamiselle. Toteutuneilla kyberturvallisuusuhilla voi olla merkittävä vaikutus organisaation talouteen ja maineeseen. (Viestintävirasto 2014, 18) IBM raportoi, että maailmanlaajuisesti yrityksillä kestää keskimäärin 207 päivää havaita tietomurto ja 73 päivää siitä palautumiseen. (IBM 2020, 52).

Kyberturvallisuuskyvykkyyttä parantavat keinot tulisi näkyä organisaation jokapäiväisessä toiminnassa. Kyberturvallisuuskypsyys edellyttää tarvittavan teknologian lisäksi sitä, että organisaation koko henkilöstö on koulutettu ja sitoutunut hyviin tietoturvallisuutta parantaviin käytäntöihin. Kyberriskien on oltava osa organisaation arjen riskienhallintaa. Jopa hyvin yksinkertaisten kyberturvallisuutta parantavien toimenpiteiden toteuttaminen auttaa vähentämään kyberhäiriöiden todennäköisyyttä tai vaikuttavuutta. Valmistautuminen kyberhäiriöiden havainnointiin ja nopeaan reagointiin auttaa rajoittamaan vahinkoja. (Traficom julkaisuja 2/2020, 15–28). Verizonin Data Breach -raportti osoittaa, että 85 % tietoturvarikkomuksista liittyy inhimillinen tekijä ja vain 3 % liittyy haavoittuvuuksien hyväksikäyttöön. (Verizon 2021, Artikkeli).

Kyberturvallisuuskyvykkyyden kehittämiseen löytyy kansainvälisiä standardeja ja viitekehyksiä, joiden avulla organisaatio voidaan luoda itselleen määrämuotoisen jatkuvaan parantamiseen pohjautuva kyberturvallisuuden hallintamallin. Kyberturvallisuuskyvykkyyden lisääntyminen tarjoaa organisaatiolle kilpailuetua, sillä asiakkaat ja yhteistyökumppanit arvostavat ja edellyttävät heidän luottamuksellisten tietojensa pysymistä turvassa. Se, että organisaatio huolehtii omasta kyberturvallisuudesta, vaikuttavat tehdyt toimenpiteet positiivisesti myös asiakkaiden ja sidosryhmien kyberturvallisuuteen. (Viestintävirasto 2014, 18)

1.1 Toimeksiantaja ja työn taustaa

Opinnäytetyön toimeksiantaja AddSecure on Euroopan johtavia tietoturvan ja kriittisten viestintäratkaisujen toimittajia. Suomessa AddSecure tarjoaa valtakunnallisesti kiinteistöturvallisuuden tiedonsiirto- ja hallintapalveluita kiinteistöjä omistaville yritysasiakkaille ja heidän palveluntuottajillensa ja on keskeisesti mukana turvallisuuteen liittyvien viranomaispalveluiden tuottamisessa. Tällaisia kiinteistöturvallisuuden järjestelmiä ovat esimerkiksi valvottavan kiinteistön paloilmoitin, rikosilmoitin, rakennusautomaatiojärjestelmä ja kulunvalvontajärjestelmä. Viime vuosien aikana mukaan ovat tulleet voimakkaasti myös asiakaskohteiden kylmä- ja energianhallintajärjestelmät, samoin kun kuvavalvontaratkaisut. (AddSecure 2021)

AddSecuren juuret ovat eri pohjoismaiden teleoperaattoreiden aikaisemmin omistamissa hälytysten siirtopalveluissa. Yritys on kasvanut yrityskauppojen kautta. Pohjoismaat ovat sen kotimarkkinat mutta yhtiö on laajentunut nopean kasvustrategian myötä myös Australiaan, Benelux-maihin, Ranskaan, Puolaan, Espanjaan, Sveitsiin, Iso-Britanniaan, Saksaan ja Yhdysvaltoihin. (AddSecure 2021)

AddSecurella työskentelee tällä hetkellä noin 1000 työntekijää eri maissa. AddSecuren osake-enemmistön omistaa eurooppalainen pääomarahasto Castik Capital. Vähemmistöomistajia ovat Abry Partners ja AddSecuren työntekijät. (AddSecure 2021)

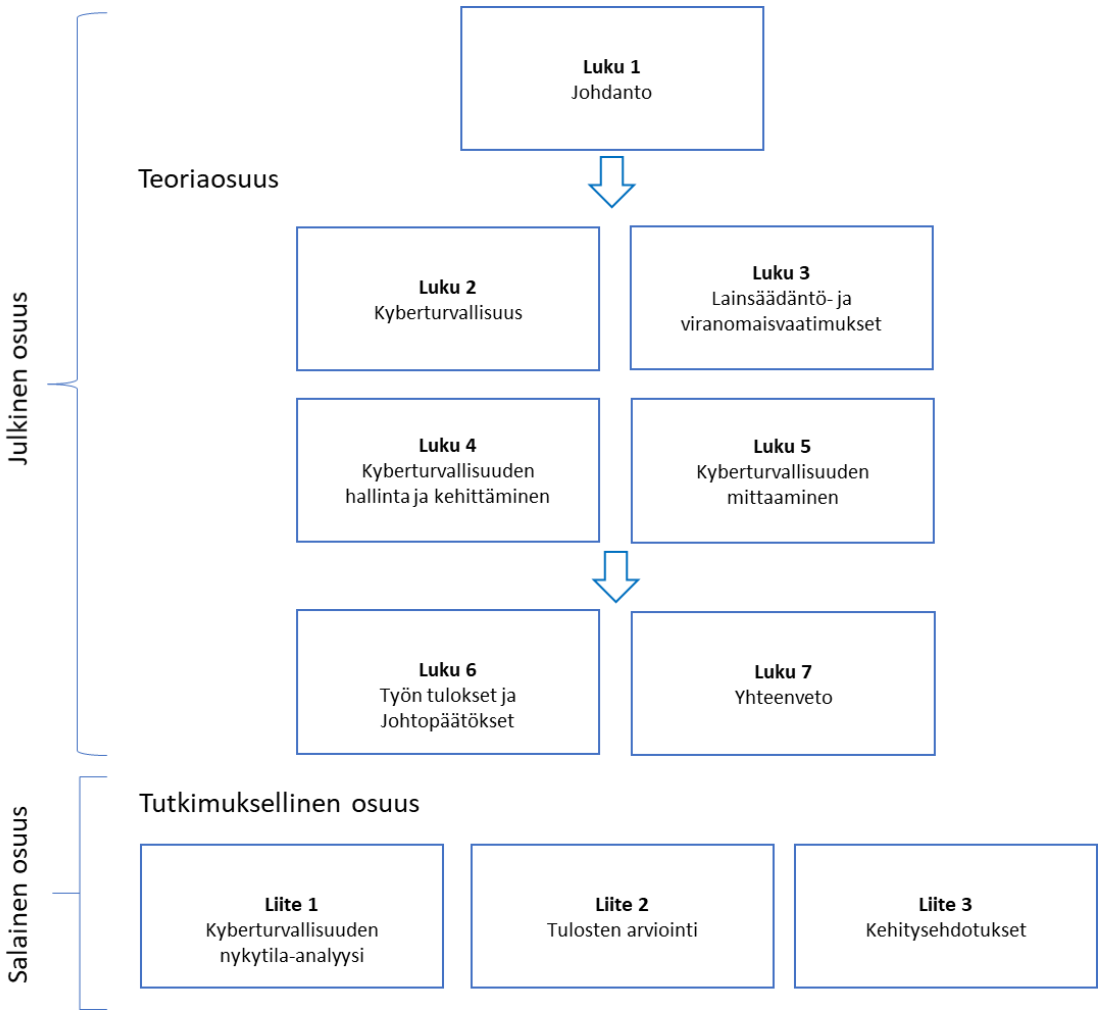
Tämän opinnäytetyön aihe syntyi tarpeesta kehittää työnantajani Suomen AddSecure Oy:n (myöhemmin AddSecure) digitaalisen turvallisuuden kyvykkyyttä luomalla organisaation kyberturvallisuuden hallintaan ja käsittelyyn jatkuvaan parantamiseen perustuva toimintamalli, jonka avulla voimme varmistaa asiakkaidemme turvallisuusvaatimukset luottamuksellisten tietojen suojaamisessa.

1.2 Työn rakenne

Opinnäytetyö jakaantuu kahteen osaa. Julkisessa osassa esitetään kyberturvallisuuteen liittyvää keskeistä teoriaa ja vaatimuksia kyberturvallisuuden hallintamallille, joiden pohjalta varsinainen kyberturvallisuuskypsyyden nykytila-analyysi ja kehitysehdotukset tehdään. Opinnäytetyön luottamuksellisuuden vuoksi analyysin tuotokset ja tarkemmat kehitysehdotukset esitetään opinnäytetyön liitteissä, ne ovat salaisia ja vain toimeksiantajan käytössä.

Tässä opinnäytetyössä noudatetaan toimintatutkimuksen periaatteita ja rakenteita. Johdantokappaleessa (luku 1) avataan aihealuetta ja kuvaillaan työn lähtökohtaa, taustaa ja ongelmakenttää. Johdannossa esitetään myös tutkimusongelmat ja rajaukset sekä työn lähestymistapa ja metodologia. Luvuissa 2 käsitellään kyberturvallisuutta osana digitaalisen turvallisuuden viitekehystä. Luvussa esitellään myös tyypillisimpiä kyberuhkia ja millainen tilanne meillä on kyberturvallisuuden osalta tällä hetkellä Suomessa. Luvussa 3 käsitellään lainsäädäntö- ja viranomaisvaatimuksia, joita viranomaisasiakkaamme edellyttävät AddSecurelta toimiessaan heidän yhteistyökumppaninansa. Luvussa käsitellään myös viranomaisten suojattavan tietoaineiston käsittelyä, luokittelua ja suojaamista ja mitkä ovat tietoturvallisuuden perustason viranomaisvaatimukset. Luvussa 4 tuodaan esille organisaation jatkuvuudenhallinnan näkökulmaa, sillä kyberturvallisuus on mitä suuremmassa määrin riskienhallintaa ja varautumista erilaisiin kyberhäiriöihin. Luvussa käsitellään myös NIST:n Cyber Security Framework (CSF) -viitekehyksen pohjalta keskeisimpiä kyberturvallisuuden hallintakeinoja, joita toteuttamalla organisaatio voi kehittää kyberturvallisuuskyvykkyyttä (tunnistaminen, suojautuminen, havaitseminen, reagoiminen ja palautuminen) kyberhäiriötilanteiden osalta. Näitä kyberturvallisuuden kehitystoimenpiteitä ei kannata tehdä yksittäin vaan niiden toteuttamisessa kannattaa hyödyntää kokonaisvaltaista lähestymistapaa. Käytännössä on havaittu, että paras tapa on luoda organisaatiolle hallintamalli, jossa kyberturvallisuus saadaan yhdistettyä työntekijöiden päivittäisiin tekemisiin, eivätkä ne ole irrallisia toimenpiteitä. Tämän kyberturvallisuuden johtamis- ja hallintamallin tulee kattaa keskeiset kyberturvallisuuden johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat toimenpiteet ja menettelytavat. Sen kehittämisessä voidaan hyödyntää useita keskeisiä kyberturvallisuustyötä tukevia viitekehyksiä. Jotta kehittämistoimintaa voidaan seurata ja ohjata, tulee sitä voida myös mitata. Luvussa 5 käsitellään kyberturvallisuuskypsyyden mittaamista. Työn viimeisissä luvuissa 6–7, esitetään tutkimuksessa saavutetut (julkaistavissa olevat) tulokset ja johtopäätökset sekä tarkastellaan työn onnistumista suhteessa tutkimuskysymyksiin. Lopuksi pohditaan työhön liittyviä jatkotoimenpiteitä, jotka muodostavat jatkumon kyberturvallisuuden hallintamallin implementoinnissa käytäntöön.

Opinnäytetyön luottamuksellisen osion liitteissä 1–2 suoritetaan organisaatiolle Kyberturvallisuuskeskuksen Kybermittarin pohjalta kyberturvallisuuden kypsyystason nykytila-arvio sekä viranomaisille tarkoitetun Katakri 2020-tietoturvallisuuden auditointityökalun avulla arvio organisaation kyvystä suojata viranomaisen salassa pidettävää tietoa. Saatujen tulosten perusteella liitteessä 3 tehdään AddSecurelle tilaajan pyytämät kehitysehdotukset kyberturvallisuuskypsyyden perustason ja Katakrin turvallisuustaso ST IV edellyttämistä jatkotoimenpiteistä. Kuvassa 1 on esitetty tutkimuksen rakenne.



Kuva 1. Tutkimuksen rakenne

1.3 Viitekehys, tavoitteet, tutkimusongelma ja aiheen rajaus

Valtionhallinnon organisaatioiden täytyy vastata yhteiskunnallisista velvoitteistaan. Keskeisenä osana tähän vastuuseen liittyy osoitusvelvollisuus tietoturvallisuuden ja tietosuojan toteutumisesta. Viranomaisen tulee huolehtia samojen velvoitteiden ja vaatimusten täyttymisestä myös heidän ulkoistaessaan toimintoja ulkopuoliselle yritykselle, esimerkiksi AddSecurelle, tai hankkiessaan heiltä palveluita. (Rousku 2014, 125–126)

Opinnäytetyön tavoitteena on luoda edellä mainitut asiakasvaatimukset täyttävän kyberturvallisuuden hallintamallin runko, johon sisältöä kehitetään jatkossa omina projekteina normaalin päivätyön puitteissa. Aikaisemman kokemuksen perusteella kyberturvallisuusprosesseista voi helposti tulla liian raskaita hoitaa, jolloin ne jäävät hoitamatta tai hoidetaan vain osittain. Yksi tämän opinnäytetyön tavoitteista on löytää kyberturvallisuuden hallintaan sellainen kultainen keskitie, jolla viranomaisasiakkaiden turvallisuusvaatimukset täytetään ja ne kyetään hoitamaan olemassa olevalla henkilöstöllä normaalien turvallisuusprosessien puitteissa.

Tässä opinnäytetyössä halutaan saada vastaukset seuraaviin tutkimuskysymyksiin:

- Mistä kyberturvallisuuden hallintamalli koostuu?
- Mitkä ovat eri viitekehysten ja standardien vaatimukset viranomaisten turvallisuusluokka ST IV:n täyttävälle kyberturvallisuuden hallintamallille?
- Mitkä kyberturvallisuuden hallintamallin prosessit ja dokumentit organisaatiolta vielä puuttuvat turvallisuusluokka ST IV:n vaatimuksiin nähden?

Vastauksia tutkimuskysymyksiin etsitään aluksi aihetta käsittelevästä kirjallisuudesta ja internetistä löytyvästä dokumentaatiosta. Tämän teoriatiedon perusteella muodostetaan syvällisempi käsitys työhön liittyvästä aihepiiristä sekä viitekehyksestä, jonka perusteella kyberturvallisuuden hallintamallin vaatimukset voidaan sitten määrittää.

Työn tilaaja AddSecure toivoo opinnäytetyön lopputulemaksi esitystä, miten organisaatiossa pystytään täyttämään kyberturvallisuuden osalta Katakri turvallisuusluokka ST IV -vaatimukset erityisesti teknisen tietoturvallisuuden osa-alueella. Kehitysehdotuksen toivottiin olevan myös mahdollisimman käytännönläheinen ja toteutuskelpoinen.

Kyberturvallisuus liittyy keskeisesti digitaaliseen turvallisuuteen. Siinä tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöihin ja niiden vaikutuksiin. Tästä syystä opinnäytetyössä kyberturvallisuuden hallintamallin kehittäminen painottuu valtaosin teknisen tietoturvallisuuden osa-alueisiin ja niiden edellyttämien vaatimusten täyttämiseen.

Onnistuessaan tämän opinnäytetyön tuotoksilla on positiivinen vaikutus organisaation kyberturvallisuuskyvykkyyden kehittymiseen ja sitä kautta yrityksen tulokseen.

1.4 Tutkimusote ja metodologia

Opinnäytetyön tutkimuksen lähestymistavan valinta liittyy kehittämistehtävän tavoitteeseen. Ojasalon, Moilasen ja Ritalahden kirjassa esitellään viisi erityyppistä lähestymistapaa:

1. Tapaustutkimuksessa tavoitteena on tuottaa tutkitun tiedon kohteesta ja siinä painottuvat tavanmukaisen tutkimuksen tavoitteet. Tapaustutkimusta voidaan käyttää hyvin lähestymistapana, kun halutaan ymmärtää perusteellisesti jonkin organisaation tilanne ja tavoitteena on tuottaa tutkimuksen keinoin kehittämisehdotuksia tai ratkaista siellä ilmennyt ongelma. Tapaustutkimuksessa kehittämisehdotuksia ei käytännössä vielä viedä eteenpäin tai kehitetä mitään konkreettista vaan sen avulla luodaan ainoastaan kehittämisideoita havaittuun ongelmaan. Tapaustutkimuksessatutkimiseen käytetään useita erilaisia tiedonhankintamenetelmiä, jotta tutkittavasta kohteesta saadaan kokonaisvaltainen kuva.
2. Toimintatutkimuksessa painottuvat samaan aikaan sekä tutkitun tiedon tuottaminen että käytännön muutoksen aikaansaaminen. Toimintatutkimuksessa keskeinen piirre on organisaatiossa toimivien ihmisten aktiivinen osallistuminen kehittämistyöhön ja siinä pyritään tyypillisesti ihmisten toiminnan muuttamiseen.

3. Konstruktiivisessa tutkimuksessa tavoitteena on ratkaista käytännön ongelma kehittämällä uusi konstruktio eli konkreettinen tuotos. Se voi olla esimerkiksi tuote, tietojärjestelmä, ohje- tai käsikirja, malli, menetelmä tai suunnitelma. Konstruktiivisessa tutkimuksessa muutos on tärkeä sitoa aikaisempaan teoriaan.
4. Palvelumuotoilussa sovelletaan muotoilun prosesseja ja menetelmiä palvelun kehittämiseen. Palvelumuotoilua voidaankin hyödyntää palvelun kehittämiseen sen elinkaaren eri vaiheissa. Uudistamisen kohteena voi olla esimerkiksi yrityksen strategia, liiketoimintamalli, prosessit tai palveluympäristö. Palvelumuotoilun avulla voidaan helposti ja nopeasti konkretisoida ja testata aineettomia palvelukonsepteja. Palvelumuotoilun tärkeä erityispiirre on eri sidosryhmien aktiivinen osallistuminen kehittämistyöhön.
5. Innovaatioiden tuottaminen ja tutkiminen on lähellä konstruktiivista tutkimusta sekä palvelumuotoilua. Innovaatiolla tarkoitetaan esimerkiksi uutta tuotetta, palvelua, prosessia tai toimintamallia, jolla organisaatiolle tuotetaan taloudellista tai muuta hyötyä. Innovaatioissa on tärkeää niiden toteuttaminen ja kaupallistaminen.

Kehittämistehtävä myös määrittää, mikä näistä lähestymistavoista soveltuu parhaiten kyseessä olevaan kehittämistyöhön, ja ne ovat yleensä osin päällekkäisiä, joten kehittämishankkeessa voi olla piirteitä useammasta lähestymistavasta. (Ojasalo, Moilanen & Ritalahti 2015, 36)

Tässä opinnäytetyössä tutkitaan aihetta, jossa pyritään muuttamaan yrityksen olemassa olevia kyberturvallisuuskäytäntöjä. Kyseessä on tapaustutkimus, kun halutaan syvällisesti ymmärtää organisaation tilanne ja tutkimuksellisesti saada aikaan kehittämisehdotuksia. Opinnäytetyössä hyödynnetään myös toimintatutkimuksen kvalitatiivisia eli laadullisia menetelmiä, koska tutkiminen kyberturvallisuuskyvykkyyden analysoinnissa osallistutetaan organisaation ihmisiä analysointiin ja kehittämiseen ja pyritään samalla muuttamaan ihmisten toimintaa.

1.5 Työn etenemisen vaiheet ja aikataulu

Opinnäytetyö toteutetaan seuraavin askelin:

1. Aluksi tutustutaan kyberturvallisuuden teoriaan ja keskeisiin viitekehyksiin. Viitekehysten pohjalta määritellään niiden parhaiden käytäntöjen perusteella kyberturvallisuuden hallintamallin sisältö ja vaatimukset.
2. Tämän jälkeen organisaatiolle tehdään nykytilan analyysi Kyberturvallisuuskeskuksen Kybermittarin sekä Katakri 2020-tietoturvallisuuden auditointityökalun avulla. Myös ISO 27001 -puuteanalyysi käydään läpi aihealueen keskeisten kohtien osalta. Analyysit kertovat mitkä asiat organisaatiolla on jo kunnossa ja mitä tulisi vielä kehittää, jotta ne täyttävät asiakkaiden edellyttämät kyberturvallisuusvaatimukset.
3. Lopuksi tehdään ehdotus jatkotoimenpiteistä, joilla saamme puuttuvat kyberturvallisuuden hallintamallin edellyttämät prosessit ja ohjeistukset kuntoon. Keskeistä olisi myös löytää muutama kyberturvallisuuteen liittyvä mittari, joilla olemassa olevaa toimintaa ja tulevaa jatkokehitystä voitaisiin seurata ja raportoida yrityksen johdolle.

4. Varsinainen kyberturvallisuuden hallintamallin edellyttämä uusi dokumentaatio, ohjeistus ja prosessit luodaan sitten omina projekteinaan opinnäytetyön jälkeen.

Kehitysprojektin suunnitelma ja aikataulu on esitetty kuvassa 2.

	Helmikuu 2021	Maaliskuu 2021	Huhtikuu 2021	Toukokuu 2021	Kesäkuu 2021	Heinäkuu 2021	Elokuu 2021	Syyskuu 2021	Lokakuu 2021	Marraskuu 2021	Joulukuu 2021	Tammikuu 2022	Helmikuu 2022	Maaliskuu 2022	Huhtikuu 2022	Toukokuu 2022	Kesäkuu 2022	Heinäkuu 2022
Opinnäytetyön alustava aikataulu	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Lopputyön aiheen valinta, suunnittelu ja anominen																	Varalla	
Teoria ja vaatimukset kyberturvallisuuden hallintajärjestelmälle. Kyberturvallisuuden hallintajärjestelmän rungon luominen parhaiden käytäntöjen pohjalta.																		
Nykytilan kartoittaminen (Kybermittari ja Katakri 2020 - tietoturvallisuuden auditointityökalu)																		
Suunnitelma/ehdotus niistä jatkotoimenpiteistä, joilla saamme puuttuvat kyberturvallisuuden prosessit ja ohjeistukset kuntoon.																		
Tulokset/Johtopäätökset																		
Lopputyön viimeistely																		
Tulosten julkaisu																		

Kuva 2. Kehitysprojektin suunnitelma ja aikataulu

2 KYBERTURVALLISUUS

Suomen kyberturvallisuusstrategia määrittää kyberturvallisuuden tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvata. Tavoitetilassa kybertoimintaympäristöstä ei koidu vaaraa sähköisestä tiedonsiirrosta riippuvaisille organisaatioille eikä niiden prosesseille. Luottamus kybertoimintaympäristöön pohjautuu siihen, että organisaatiot suorittavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä eli hallintatoimenpiteitä, joiden avulla voidaan estää tietoturvauhkien toteutuminen tai niiden toteutuessa estämään, lieventämään ja sietämään niiden vaikutuksia. Kyberturvallisuus siten pitää sisällään kriittiseen infrastruktuuriin kohdistuvat hallintatoimenpiteet, joiden avulla pyritään saamaan kyvykkyys ennakoivasti hallita ja tarvittaessa myös sietää kyberuhkia ja niiden vaikutuksia. (Turvallisuuskomitean sihteeristö 2013, 13)

Kyberturvallisuus keskittyy tietoteknisten järjestelmien turvaamiseen ja pääpaino on tietoverkoissa, joista on yhteys internettiin. Useimmat toteutuneet kyberturvallisuuden pettämiset liittyvät internetin kautta tehtäviin kyberhyökkäyksiä. Hyökkäysten avulla on onnistuttu heikentämään tietoturvallisuutta muuttamaan tietojen sisältöä, loukattu yksityisyyden suojaa vuotamalla henkilötietoja tai haitattu organisaation palveluiden käytettävyyttä palvelunestohyökkäyksen avulla. (Rousku 2014, 57)

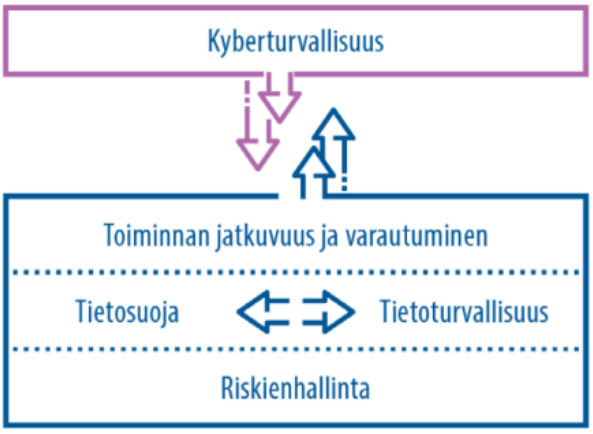
Kyberturvallisuutta pidetään monessa yhteydessä digitaalisen turvallisuuden synonyyminä. Tänä päivänä digitaalinen toimintaympäristö ja sen turvallisuus on keskeinen osa kaikkien organisaatioiden toimintaa. Digitaalinen turvallisuus tukee osaltaan organisaation mahdollisimman häiriötöntä toimintaa osana muita turvallisuusratkaisuja.

2.1 Kyberturvallisuus on osa digitaalisen turvallisuuden viitekehystä

Kyberturvallisuuden toteutuminen edellyttää tietojen saatavuuden, eheyden ja luottamuksellisuuden toteuttamista eli tietoturvallisuudesta huolehtimista. Organisaation toimintojen suojaaminen vaatii ennalta proaktiivista varautumista ja häiriöiden tapahtuessa ennakkoon laadittujen suunnitelmien mukaista aktiivista toimintaa eli toimintojen jatkuvuudesta ja varautumisesta huolehtimista. Organisaation käsittelemä tieto voi olla henkilötietoa, joka tästä syystä edellyttää tietosuojasta huolehtimista. Kaiken edellä kuvatun tulisi perustua toimintatapaan, johon kuuluu uhkien tunnistaminen, riskien arvioiminen ja niihin perustuva suunnitelmallinen riskienhallinta. (Digi- ja väestötietovirasto 2021, 6)

Digitaalisen turvallisuuden viitekehys koostuu seuraavista osa-alueista:

1. Riskienhallinta
2. Toiminnan jatkuvuus ja varautuminen
3. Tietoturvallisuus
4. Tietosuoja
5. Kyberturvallisuus (Digi- ja väestötietovirasto 2021, 6)



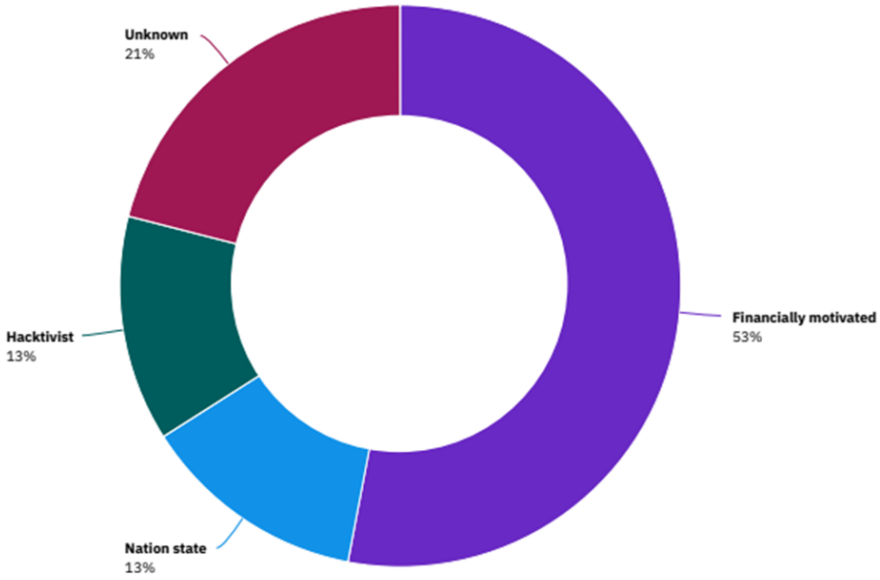
Kuva 3. Digitaalinen turvallisuus koostuu viidestä osa-alueesta. (Väestörekisterikeskus 2019, 15)

Kehittämällä samanaikaisesti riskienhallintaa, toiminnan jatkuvuutta ja varautumista, tietoturvaa ja tietosuojaa, edistetään samalla kyberturvallisuutta, sekä organisaation että yhteiskunnan tasolla. (Digi- ja väestötietovirasto 2021, 28)

2.2 Organisaatioon kohdistuvia kyberuhkia

Ciscon toimitusjohtaja John Chambers sanoo, että "On olemassa kahdenlaisia yrityksiä: niitä, jotka on hakkeroitu, ja niitä, jotka eivät vielä tiedä, että heidät on hakkeroitu". Kyberuhka on toteutuessaan haitallinen tapahtuma, joka kohdistuu kybertoimintaympäristöön vaarantaen siihen liittyvät toiminnot. Kyberuhat voivat syntyä esimerkiksi toteutuneista tietoturvauhkista ja ne voivat kohdistua suoraan tai epäsuoraan yhteiskunnan elintärkeitä toimintoja, kriittistä infrastruktuuria tai yksittäistä kansalaista vastaan. Kyberuhat voivat olla peräisin kotimaasta tai ulkomailta. (Traficom 2020 3, 3).

Kyberrikollinen ei käytä murtautuessaan fyysisiä voimakeinoja, vaan se tunkeutuu esimerkiksi organisaation tietojärjestelmiin internetin kautta ja varastaa sieltä tietoa. Kyberhyökkäyksessä voidaan hyödyntää haittaohjelmien levittämisessä kohteen kriittisten ohjausjärjestelmien heikkouksia, jolloin haittaohjelmalla voidaan lamauttaa esimerkiksi voimalaitoksen toiminta tai sähkönjakelu. Kyberturvallisuutta uhkaaviin tekijöihin ovat myös erilaiset luonnonilmiöt. Myrskyt tai muut luonnonilmiöt voivat vaurioittaa niin sähkö- kuin tietoliikennekaapeleita. Koko digitaalinen yhteiskunta on riippuvainen toimivasta tietoliikenneinfrastruktuurista, joka taas tarvitsee toimiakseen varmistettua sähköä. Laajamittaiset tietoliikennehäiriöt voivat estää tai haitata lukuisten organisaatioiden tarjoamia palveluita ja toimintoja. (Digi- ja väestötietovirasto 2021, 28) IBM raportoi kuvan 4 mukaisesti, että yli puolessa tietomurroista päämotiivina on taloudellinen hyötyminen.



Kuva 4. Tietomurtojen uhkatyypit 2021 (IBM 2020, 27).

Tyypillisimpiä kyberuhkia ovat tietojenkalastelu, haittaohjelmat, kiristysohjelmat ja palvelunesto-hyökkäykset. (Traficom julkaisuja 228/2020, 4–8) (Traficom julkaisuja 2/2020, 4)

2.2.1 Tietojenkalastelu

Tietojenkalastelussa murtautujan päämääränä on saada haltuun henkilön käyttäjätunnus ja salasana tai muita organisaatiolle merkityksellisiä tietoja. (Traficom julkaisuja 2/2020, 4) Käyttäjä voi saada esimerkiksi sähköpostissa houkuttelevan tarjouksen tai mahdollisuuden osallistua kilpailuun. Jotta hän voi nostaa saadun voiton tai hyödyntää edullisen tarjouksen, pitää sivustolle antaa usein henkilö- tai maksukorttitietoja. Täältä ne päätyvät sitten rikollisten haltuun. CSO Onlinen artikkelin mukaan 94 % tietojenkalastelusta tapahtuu sähköpostin välityksellä. (Ccoonline, Artikkeli). Käyttäjien tulisi tunnistaa tietojenkalasteluviestit, ja poistaa ne sähköpostista niitä avaamatta. (Turvallisuuskomitea 2017, 20)

2.2.2 Haittaohjelmat

Haittaohjelmat ovat tietokoneohjelmia, jotka tarkoituksellisesti aiheuttavat tietojärjestelmän tai laitteen käyttäjän kannalta haitallisia tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat muun muassa virukset, madot ja troijalaiset sekä näiden yhdistelmät. (Traficom julkaisuja 2/2020, 7) Tavallisesti haittaohjelman voi saada, kun lataa videoita, kuvia tai ohjelmia arveluttavilta nettisivuilta. Nykyään haittaohjelma voi siirtyä käyttäjien tietokoneille myös luotettavina pidetyiltä nettisivuilta. (Turvallisuuskomitea 2017, 19)

2.2.3 Kiristysohjelmat

Kiristyshaittaohjelman eli ransomwaren voi saada tietokoneelle esimerkiksi, kun lataa ilmaisen ohjelman tai avaa sähköpostissa liitetiedoston, johon haittaohjelma on piilotettu. (Turvallisuuskomitea

2017, 19) Kiristyshaittaohjelma latautuu koneelle, kun käyttäjä avaa sähköpostin liitetiedoston. Tämän jälkeen kiristysohjelma muuntaa organisaation tiedostoja salakirjoitettuun muotoon ja näitä tiedostoja ei voi avata ilman oikeaa salauksenpurkuavainta. Kiristysohjelma näyttää tietokoneen käyttäjälle ilmoituksen, jossa vaaditaan lunnaiden maksamista tietokoneen lukituksen poistamiseksi. Näiden kiristysohjelmien lunnasvaatimukset ovat usein summiltaan alle 1000 € suuruisia, koska rikolliset uskovat tällaisten summien olevan käyttäjille helposti maksettavissa. (Opsec 2021) Kiristyshaittaohjelma voi myös uhata paljastaa luottamuksellista tietoa organisaatiosta tai käyttäjästä. Kiristysohjelman uhriksi voi joutua myös organisaatiot, joilla kyberturvallisuuden hallinta on hyvällä tasolla. Yle uutisoi helmikuussa 2022, kuinka Savonia-ammattikorkea koulu joutui kiristyshaittaohjelman kohteeksi ja sen seurauksena verkkolevyillä sijainneita tiedostoja oli lukittu ja niiden avaamiseksi vaaditaan Bitcoin-lunnaita. (Yle 2022, Artikkeli)

2.2.4 Palveluestohyökkäykset

Palveluestohyökkäyksessä organisaation tietoverkkoa kuormitetaan ylimääräisellä tietoliikenteellä. Tavoitteena on ylikuormittaa ja siten lamaannuttaa jokin organisaation palvelu tai tietojärjestelmä. Palvelunestohyökkäys voi esimerkiksi lamaannuttaa jonkun palvelimen tai reitittimen liian suurella määrällä palvelupyyntöjä. Jos palvelunestohyökkäys tulee yhdestä IP-osoitteesta, se on helppo havaita ja torjua esimerkiksi palomuurilla. Tästä syystä palvelunestohyökkäys on tyypillisesti hajautettu palvelunestohyökkäys, eli se toteutetaan yhtä aikaa useista eri lähteistä. Hajautettuun palvelunestohyökkäykseen käytetään usein hyökkääjän haltuunsa ottamista tietokoneista muodostuvaa bottiverkkoa. (Traficom julkaisuja 2/2020, 8) Kaappaushaittaohjelman voi saada myös avaamalla epämääräisen sähköpostin liitetiedoston. Ohjelma voi tulla myös internetistä ladattavan ilmaisohjelman kylkiäisenä. (Turvallisuuskomitea 2017, 20)

2.3 Haittaohjelmahyökkäyksen kohteeksi joutumisen syitä

Kaikilla yrityksillä on hallussaan tietoa, osaamista ja erilaisia tietojärjestelmiä, joista ulkopuolinen voi hyötyä. Organisaation on itse tunnistettava omat suojattavat kohteensa. Organisaation on myös hyvä ymmärtää, että hyökkäyksen voi mahdollistaa myös sen puutteellinen havainnointikyky, joka laukaisisi oikea-aikaiset vastatoimenpiteet havaittuun hyökkäykseen reagoimiseksi. (Viestintävirasto 2014, 7)

Hyökkäykselle altistavia syitä ovat:

1. Organisaation kiinnostava informaatio
2. Organisaation merkittävät yhteistyökumppanit.

Hyökkäyksen torjumisen hankaloittavia syitä ovat:

3. Verkon ja järjestelmien teknisesti tarjoamat mahdollisuudet
4. Puutteet hyökkäysten havainnointi- ja reagointikyvyssä.

Kuva 5. Syitä organisaatioon kohdistuvan haittaohjelmahyökkäyksen uhkaan (Viestintävirasto 2014, 8)

Mitä useampi yllä olevista hyökkäykselle altistavista tekijöistä tai hyökkäyksen mahdollistavista tekijöistä toteutuu, sitä suurempi mahdollisuus on, että organisaatio joutuu haittaohjelmahyökkäyksen uhriksi. Haittaohjelmahyökkäyksen kohteeksi voi silti joutua, vaikka kaikkiin osa-alueisiin olisi kiinnitetty huomiota.

2.4 Haittaohjelmahyökkäyksen toteutus

Haittaohjelmahyökkäyksiltä suojautumista auttaa, jos ymmärtää haittaohjelmahyökkäyksen toteutusvaiheita ja niissä käytettäviä tapoja. Yleensä hyökkääjä arvioi kuitenkin toteutuksen ja sen vaatiman panostamisen kustannustehokkuutta sekä hyökkäyksen paljastumiseen riskiä. Kuvassa 6 on kuvattu tyypillisen hyökkäyksen päävaiheet. (Viestintävirasto 2014, 10)

Kuva 6. Toteutuksen vaiheet (Viestintävirasto 2014, 10)

Haittaohjelmahyökkäystä ja varsinkin kohdistettu hyökkäystä valmistellaan yleensä huolella. Kohdeorganisaatiosta kerätä julkisista lähteistä niin sosiaalisia kuin teknisiä tietoja. Näitä tietoja hyödynnetään hyökkäyksen seuraavissa vaiheissa. Teknisiä tietoja käyttämällä yritetään ohittaa verkon havainnointijärjestelmät, hyödyntämällä kohdeverkon järjestelmien ja ohjelmistojen sisältämät haavoittuvuudet ja konfiguraatiovirheet. (Viestintävirasto 2014, 10)

Tunkeutumisessa hyödynnetään kohdeorganisaatio päivittäisiä työmenetelmiä. Hyökkääjä lähettää esimerkiksi kohteellensa sähköpostin ja houkuttelee kohteen luomilleen nettisivuille mielenkiintoa herättävällä sisällöllä. Hyökkääjä selvittää myös, mitä ohjelmistoja kohde käyttää ja etsii niistä haavoittuvuuksia. Tehokkaimpia ovat tuoreet ohjelmistoyritysten julkisesti ilmoittamat 0-päivähaavoittuvuudet, joita kohdeorganisaatioissa ei ole vielä pystytty päivittämään ajantasaisiksi ei saatavissa olevan ohjelmistopäivityksen puutteen takia. (Viestintävirasto 2014, 11)

Jotta hyökkääjä saisi pysyvän aseman kohteen tietoverkossa ja -järjestelmissä, sisään saatu haittaohjelma pyritään levittämään nopeasti riittävän moneen paikkaa, jotta se ei häviä sieltä vaikka joitakin saastuneita koneita vaihtuisi tai poistuisi verkosta. Hyökkääjä voi asentaa kohteensa verkkoon myös pysyvän jalansijan eli takaoven. Tämä tapahtuu esimerkiksi lisäämällä itselle pääsytunnukset järjestelmään tai asentamalla haittaohjelma, jonka avulla hyökkääjän on mahdollista ottaa etäyhteys ja ohjata verkon päätelaitteita. (Viestintävirasto 2014, 12)

Piiloutuminen ja jälkien siivoaminen on oleellinen osa hyökkäystä, jotta kohdeverkko- tai järjestelmään olisi mahdollista palata myös myöhemmin. Näkyvät merkit käynnistä pyritään poistamaan, jotta lokeista ei paljastuisi viitteitä meneillään olevasta tai menneestä laittomasta verkkohyökkäyksestä. (Viestintävirasto 2014, 13)

2.5 Kyberhäiriön vakavuus

Yksi keskeisimmistä huomiotta jätetyistä asioista on määritellä, mitä kyberuhkalla tai tietoturvapoikkeamalla tarkoitetaan. Siihen liittyy kolme eri näkökohtaa:

- Miten kybertapahtuma tai poikkeama havaittiin ja sai alkunsa?
- Missä vaiheessa siitä kehittyy kyberhäiriö tai tietoturvaloukkaus?
- Missä vaiheessa siitä tulee niin vakava häiriö, että se edellyttää normaaliprosessista poikkeavia toimintamalleja? (Traficom julkaisuja 2/2020, 37).

Kuvissa 7 ja 8 on esitetty poikkeaman vakavuuden ja tyypin luokittelut. Ne ovat hyvä sovittaa organisaation omaan riskienarviointiin.

Vakavuusaste	Kuvaus
Ei poikkeamaa	Havainto selvitetty eikä sen yhteydessä tunnistettu poikkeamaa.
Vähäinen	Poikkeaman vaikutus organisaation toimintaan on vähäinen. Vähäisten tietoturvapoikkeamien hoitaminen on osa organisaation normaalia toimintaa. Poikkeamasta voi harkinnan mukaan ilmoittaa Viestintäviraston Kyberturvallisuuskeskukseen.
Tavanomainen	Poikkeamalla on vaikutuksia organisaation toimintaan, mutta sen vaikutukset kyetään poistamaan tehostetulla normaalitoiminnalla ja seurannalla. Poikkeamasta voi ilmoittaa Viestintäviraston Kyberturvallisuuskeskukseen.
Vakava	Poikkeamalla on merkittävä vaikutus organisaation toimintaan ja tietoturvapoikkeamien käsittelyryhmä kutsutaan koolle. Poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen.
Kriittinen	Kyseessä on laaja-alainen tai organisaatiorajat ylittävä poikkeama. Organisaation sisäiset kriisinhallintatoimenpiteet käynnistetään ja poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen. Kyberturvallisuuskeskus ja kohdeorganisaatiot arvioivat, kutsutaanko koolle VIRT-koordinointikokous. Myös toimivaltainen viranomainen voi kutsua VIRT-kokouksen koolle.

Kuva 7. Poikkeaman vakavuusasteen luokittelu (Valtiovarainministeriön julkaisuja 8/2017, 36)

Poikkeamaluokka	Poikkeamatyyppi	Esimerkki
Tiedon saatavuus-ongelma	Palvelunestohyökkäys	Saatavuusongelmat voivat johtua erilaisista palvelunestohyökkäyksistä tai esim. sähkönsyöttöön liittyvistä ongelmista.
	Sabotaasi	
	Sähkökatkos	
Tietoaineisto-turvallisuus	Luvaton pääsy tietoon	Tietoaineistoon liittyvät poikkeamat voivat liittyä mm. käyttäjätilin tai sovelluksen murtamiseen, verkon nuuskimiseen tai virheellisen konfigurointiin
	Tietojen luvaton muokkaus	
Petos	Palvelujen laiton käyttö	Palvelujen käyttö laittomaan tarkoitukseen
	Tekijänoikeusrikkomus	Lisensoimattoman sovelluksen asentaminen tai myyminen
	Toisena henkilönä esiintyminen	Identiteettivarkaudet
	Tietojen kalastelu	Salassa pidettävän tai sensitiivisen tiedon kalastelu
Haavoittuvuus	Järjestelmä on avoin väärinkäytölle	Järjestelmässä on paikkaamattomia haavoittuvuuksia tai järjestelmä on konfiguroitu virheellisesti
Joku muu	Kaikki muut poikkeamat, jotka eivät sovi muihin luokkiin	

Kuva 8. Poikkeamatyypin luokitteluesimerkki (Valtiovarainministeriön julkaisuja 8/2017, 38)

2.6 Kyberturvallisuuden nykytila Suomessa ja maailmalla

Kyberturvallisuuskeskuksen kuukausittain julkaisema kybersääkooste kertoo menneen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Se on erityisesti suunnattu tietoturvasta vastaaville henkilöille, mutta arjen kyberturvallisuus -osiossa on hyviä neuvoja myös tavalliselle kansalaiselle. Kybersääkoosteesta saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. (Traficom 2021, Artikkeli) Kybersään tilanne tiivistetään sivulla kolmella tavalla.

Sää on poutainen, jolloin tilanne on rauhallinen, sää on pilvinen, jolloin tilanne on huolestuttava ja jos sää on myrskyisä, niin tilanne on vakava

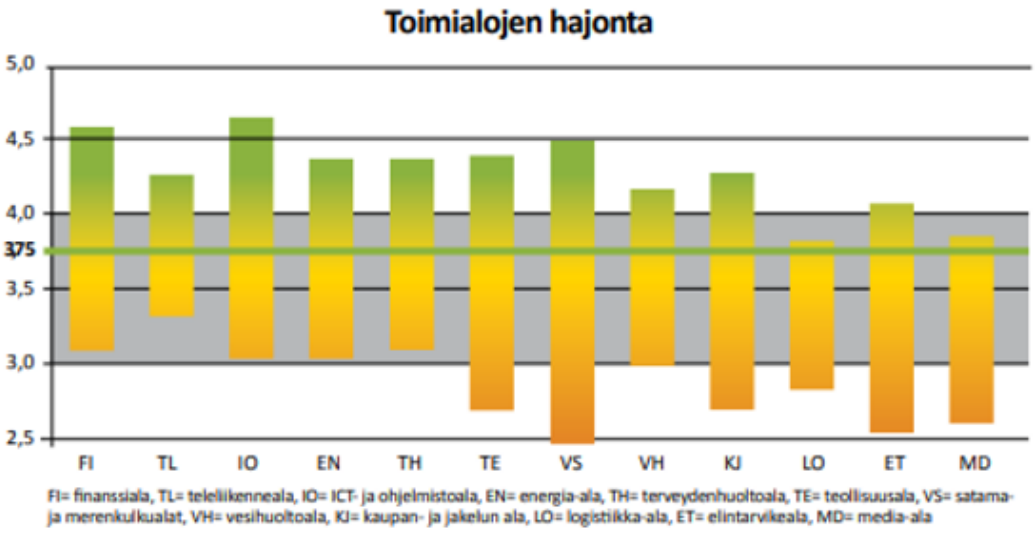
Kuva 9. Suomen kybersää lokakuussa 2021 (Traficom 2021, Artikkeli)

Huoltovarmuuskeskus selvitytti vuosina 2019–2020 Suomen kyberturvallisuuden nykytilan 12 toimialalla yhteistyössä Digipoolin ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa. Tuloksena saatiin kyberturvallisuuden ohjaamisen ja johtamisen yleinen ja toimialakohtainen nykytila Suomessa. Kartoituksessa painotettiin erityisesti liiketoimintariskien näkökulmaa. Yksi tärkeimmistä tuloksista oli kuvassa 10 listatut merkittävimmät kehityskohteet, jotka koskivat lähes kaikkia toimialoja.

Kuva 10. Eri toimialojen kehityskohteet (Huoltovarmuuskeskus 2020, 9)

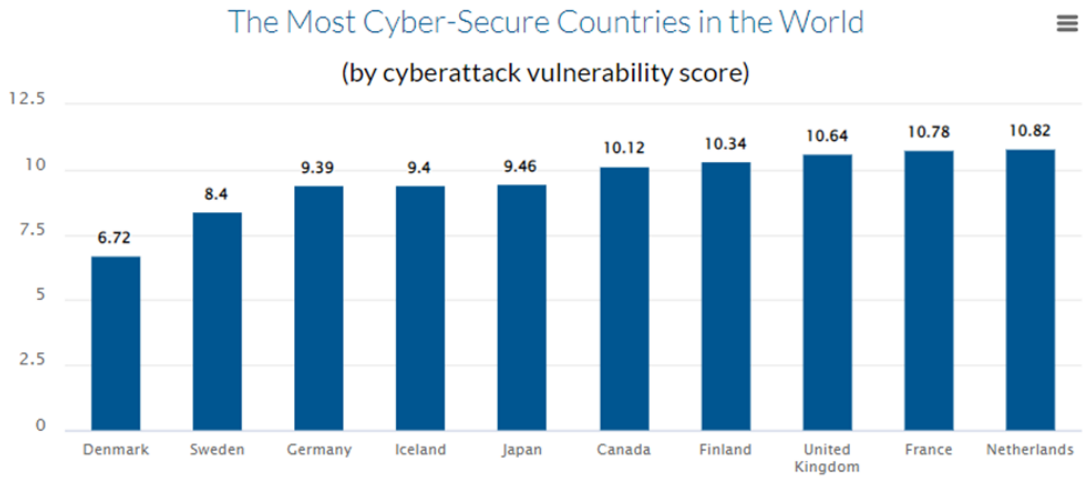
Positiivisiakin löydöksiä tehtiin. Monet yritykset osaavat esimerkiksi huomioida tekemisissään sopimuksissa erilaisia jatkuvuudenhallinnan vaatimuksia. Sopimuksiin kirjataan varsin yleisesti toimenpiteitä palvelun jatkamiseksi myös häiriötilanteissa.

Kuvassa 11 on esitetty selvityksessä kartoitettujen yritysten kyberturvallisuuden kypsyystasojen vaihteluvälit toimialoittain. Esimerkiksi teleliikennealan (TL) yritykset tekivät kyberturvallisuuteen liittyvää työtä varsin johdonmukaisesti. Toisaalta esim. satama- ja merenkulkualalla (VS) yritysten väliset tasoerot olivat suurempia, sillä osa yrityksistä kehittää kyberturvallisuutta johdonmukaisesti, mutta heikoimmat vain osittain.



Kuva 11. Toimialojen hajonta (Huoltovarmuuskeskus 2020, 8)

Financesonlinen tilastojen mukaan kuvassa 12, Suomi on yhä yksi kyberturvallisimmista maista maailmassa. ETLA kuitenkin raportoi, että Suomi ei ole kyberturvallisuuden kehityksen kärjessä, vaikka olemme vielä eurooppalaisella tasolla keskitason yläpuolella. Erityisesti tietovuodot aiheuttavat kotimaisille yrityksille yllättävän paljon haasteita. Suomea kyberturvallisuutta vaivaa myös akuutti osaamisvaje. Tällä hetkellä jopa 60 % suomalaisista kyberturva-alan yrityksistä raportoi pulaa huippuosaajista. (ETLA 2020)



Kuva 12. Maailman kyberturvallisimmat maat 2021. (FINANCESONLINE 2021, Artikkeli)

Euroopan unionin kyberturvallisuus yksikkö Enisan julkaiseman Enisa Threat Landscape 2021 -raportti mukaan yleisimmät kyberuhat Euroopassa vuonna 2021 olivat:

- Ransomware (Kiristyshaittaohjelma)
- Malware (Haittaohjelmat)
- Cryptojacking (Kryptovaluutan louhimiseen kaapattu tietokone)
- E-mail related threats (Sähköpostiin liittyvät uhat)
- Threats against data (Tietoihin kohdistuvat uhat)
- Threats against availability and integrity (Käytettävyyttä ja eheyttä uhkaavat uhat)
- Disinformation – misinformation (Väärää tietoa)
- Non-malicious threats (Ei-haitalliset uhat)
- Supply-chain attacks (Toimitusketjuhyökkäykset)

(Enisa 2021, 4)

3 LAINSÄÄDÄNTÖ- JA VIRANOMAISVAATIMUKSET

3.1 Lainsäädäntöön ja asiakassopimuksiin perustuvat vaatimukset

Suomen laki, asetukset ja EU velvoittavat organisaatioita huolehtimaan tietoturvallisuudesta, samoin kuin sopimukset muiden yhteistyötahojen kanssa. Sopimukset velvoittavat organisaatiota huolehtimaan niin omista luottamuksellisista tiedoista kuin muiden organisaatioiden ja asiakkaiden tiedoista. Tällaisen yritysten välisen turvallisuussopimuksen rikkominen voi johtaa rahallisiin sanktioihin ja jopa sopimuksen purkamiseen. (Rousku 2014, 125–126), (Suomidigi 2012, 12) Kuvassa 13 on kuvattu organisaation tietoturvallisuuteen vaikuttavia tekijöitä.

Kuva 13. Organisaation tietoturvallisuuteen vaikuttavat tekijät. (Suomidigi 2012, 12)

Viranomaisen pitää vastata kaikkien turvallisuus velvoitteiden täyttymisestä myös ulkoistaessaan toimintojaan tai hankkiessaan toimintojaan palveluina. Näille yhteistyökumppaneille tulee kohdistaa samat turvallisuus vaatimukset kuin viranomaisella on itselläkin tietoteknisen ympäristön toteuttamisessa.

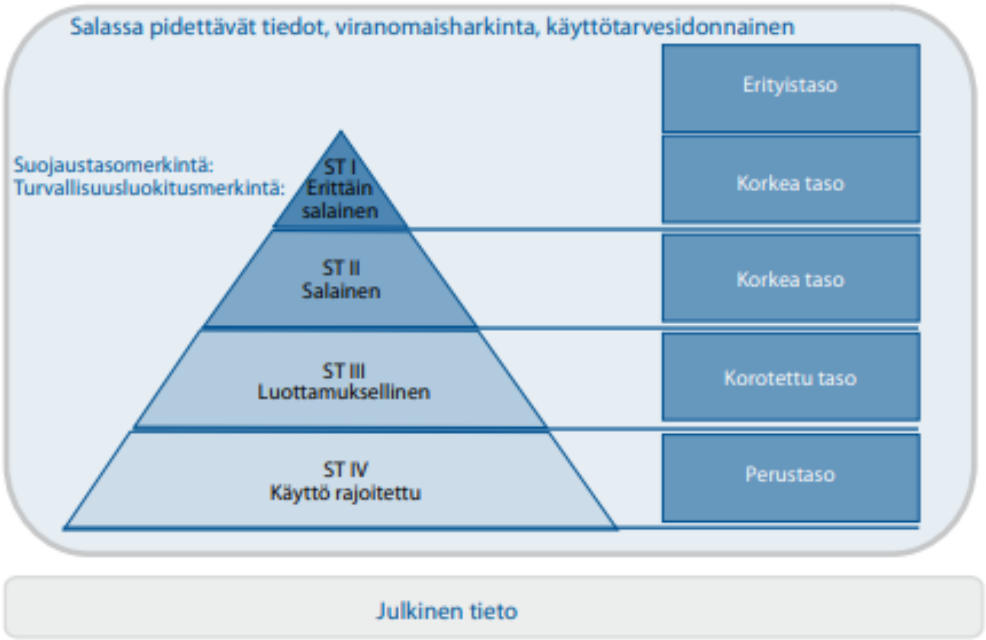
Julkisuuslain mukaisesti viranomainen voi antaa ulkoiselle yhteistyökumppanille tiedon salassa pidettävästä asiakirjasta toimeksiannon suorittamista varten. Tällöin on kuitenkin ennalta varmistettava se, että tietojen salassapidosta ja suojaamisesta huolehditaan ulkoisen toimijan toimesta asianmukaisesti. Viranomaisen on varmistuttava, että ulkoinen yhteistyökumppani, jolle salassa pidettävää tietoa luovutetaan, noudattaa Suomen tietoturvallisuusasetuksen velvoitteita. Yksityisen yrityksen osalta tietoturvavelvoitteiden noudattaminen voidaan todentaa viranomaisen harkinnan mukaan esimerkiksi ulkoisella arvioinnilla tai yrityksen omalla itsearvioinnilla, huomioiden salassa pidettävien tietojen määrä ja suojaustaso.

3.2 Tietoaineiston käsittely ja luokittelu

Organisaation tietoturvallisuuden tärkeimpiä tehtäviä on tiedon turvaaminen työpaikalla, niin toimistolla kuin etätöissä kotona. Jos työntekijä ei kykene erottamaan julkista ja salassa pidettävää tietoaineistoa, tapahtuu todennäköisesti virheitä. Pahimmillaan julkista tietoa käsitellään ja suojataan kuten salassa pidettävää, ja vastaavasti salassa pidettävää saatetaan käsitellä kuten julkista tietoaineistoa. Vaarana on, että tieto päätyy sellaisille osapuolille, joille se ei ole tarkoitettu. Samasta syystä pitää pystyä luokittelemaan salassa pidettävät tietoaineistot eri suojaustasoihin. (Rousku 2014, 68) Kun yritysten työntekijät työskentelevät nyt enemmän etätöissä, hakkereiden käytettävissä on enemmän hyökkäysvektoreita. Cybertalkin artikkelin mukaan alle 3 % organisaatioista suojaa työntekijöidensä mobiililaitteita, vaikka niillä myös saatetaan käsitellä luottamuksellisia dokumentteja esimerkiksi sähköpostin kautta. (Cybertalk 2021, Artikkeli).

Cyberintin raportin mukaan 95 % organisaatioiden kyberturvallisuusloukkauksista johtuu inhimillisestä erehdyksestä. (Cybinsolutions 2022, Artikkeli). Organisaation tulee järjestää työntekijöillesi asianmukainen tietoturvakoulutus vähentääkseen organisaatioon kohdistuvan tietomurron todennäköisyyttä. Usein sanotaan, että ihminen on heikoin lenkki, joten työntekijöihin tulee panostaa samalla tavalla kuin teknologiaan kehitettäessä organisaation kyberturvallisuuskyvykkyyttä.

Suojaustaso- tai turvallisuusluokitusmerkinnän sisältävän materiaalin käsittely edellyttää niin käsittelyn kuin sähköisen ympäristön osalta kyseessä olevan tietoturvatason vaatimusten täyttämistä. Kuvassa 14 on esitetty salassa pidettävien tietojen suojaustasomerkinnät.



Kuva 14. Tiedon suojaustasot (Suomidigi 2012, 27)

Suojaustasot on virallisesti määritetty Vahti-dokumentaatiossa kuvan 15 mukaisesti.

Suojaustasot ovat:

- suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle
- suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleiselle tai yksityiselle edulle tai, jos kysymys on tietoturvallisuusasetuksen 9 §:n 2 momentissa tarkoitetuista asiakirjoista, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Kuva 15. Tietoaineiston luokittelu (Suomidigi 2012, 27)

Tietoturvallisuuden keskeisin päämäärä on tukea organisaation toimintaa ja asetettujen tavoitteiden täyttymistä varmistamalla käsiteltävän aineistojen luottamuksellisuus, eheys ja saatavuus. Tämä onnistuu vain sillä, että aineiston käsittelyyn liittyvät tietoturvallisuus asiat huomioon kaikissa sen elinkaaren vaiheissa.

3.3 Tiedon suojaaminen

Tietoturvallisuus on yksinkertaisuudessaan organisaatiossa käsiteltävän tiedon suojaamista. Suojausta voidaan toteuttaa niin hallinnollisilla toimenpiteillä kuin teknisillä ratkaisuilla. Suojaustoimenpiteet tulee mitoittaa aina kohteen merkityksen mukaa ja suojauksen arvioinnissa tulee hyödyntää riskienhallintaa. Vaikka tietoaineiston luottamuksellisuuteen liittyisi tiukkojakin vaatimuksia, tulee tietoaineiston saatavuus myös huomioida, eli tietoa pitää pystyä myös hyödyntämään vaaditusta suojauksesta huolimatta.

Kuva 16. Tiedon suojaaminen (Suomidigi 2012, 13)

Suojattavaa tietoa säilytetään tyypillisesti tietokannassa tai palvelimelle tallennettuna. Jotta tätä tietoa voidaan helposti hyödyntää, edellyttää organisaatiolta myös muita teknisiä ratkaisuja ja tiloja, jotka pitää suojata samalla tavalla vastaamaan halutun suojaustason vaatimuksia.

Suojattavan tiedon käyttäjällä on suuri rooli tietoturvallisuuden toteutumisessa. Organisaation kannalta tehokkain ja halvin tapa parantaa tietoturvallisuutta on lisätä henkilöstön osaamista tietoturvallisuuden eri osa-alueilla.

Tiedon suojaamiseen liittyvät vaatimukset painottuvat organisaation toimintatapoihin, prosesseihin ja käytäntöihin sekä tietojärjestelmien hallintaprosesseihin. Näitä tietoturvallisuuden vaatimusten parantamistoimenpiteitä ei kannata tehdä yksittäin vaan niiden toteuttamisessa kannattaa hyödyntää kokonaisvaltaista lähestymistapaa. Käytännössä on havaittu, että paras tapa on luoda organisaatiolle tietoturvallisuuden hallintamalli, jossa tietoturvallisuus saadaan yhdistettyä työntekojöiden päivittäisiin tekemisiin, eivätkä toimenpiteet ole irrallisia toimenpiteitä.

3.4 Tietoturvallisuuden perustason vaatimukset

Tietoturvallisuusasetuksen 5 §:ssä on määritetty viranomaisille suojattavan tiedon käsittelyyn tietoturvallisuuden perustason vaatimukset. Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava kuvan 17 mukaisen tietoturvallisuuden perustason toteutumisesta.

5 § Tietoturvallisuuden perustason toteuttaminen

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

1) viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2) viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3) asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4) tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5) asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6) tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7) asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8) henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9) henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10) annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Kuva 17. Tieturvallisuuden perustason vaatimukset (Suomidigi 2014, 59).

3.5 Toimittajien jatkuvuudenhallinta vaatimukset

Viranomaisen tulee myös huolehtia, että heidän keskeiset palveluntuottajansa ovat kuvanneet viranomaisille tarjottavan palvelun osalta toimintamallit ja vastuut häiriötilanteissa. Palvelutuottajalla pitää tämän lisäksi olla palvelun osalta jatkuvuuden hallintamalli ja siihen liittyvät jatkuvuussuunnitelmat olemassa. Heidän on täytettävä myös palvelutuotannolle asetetut toiminnan jatkuvuuden ja varautumisen vaatimukset. Viranomainen hyväksyy nämä menettelytavat sekä tekniset ratkaisut ja valvoo niiden toteutumista. Palveluntuottajien on otettava myös huomioon palveluun liittyvät ylläpitovelvoitteet, resurssit sekä varaosien saatavuus häiriötilanteissa palvelujen luonteen vaatimalla tavalla. (Valtiovarainministeriö 2016, 56)

4 KYBERTURVALLISUUDEN HALLINTA JA KEHITTÄMINEN

Kyberturvallisuuden hallintaan ja kehittämiseen kuuluvat ne jatkuvuuden hallintaa tukevat toimenpiteet, joilla organisaatio voi ennakoivasti valmistautua hallitsemaan ja sietämään erilaisia kyberuhkatilanteita ja niiden vaikutuksia. Tavoitteena on, että organisaatio havaitsee mahdolliset kyberuhat, reagoi niihin nopeasti ja tarkoituksenmukaisesti ja toipuu niistä suunnitelmallisesti. Kyberuhkien hallinta on riskienhallintaan perustuvaa turvallisuuden kehittämistä ja sen keskiössä ovat kaikki organisaation digitaalisen turvallisuuden osa-alueet. (Traficom 2020 3, 3)

4.1 Toiminnan jatkuvuuden hallinta

Organisaation jatkuvuuden turvaaminen on strateginen kysymys ja hallittu kriisitilanteista toipuminen jakaa organisaatiot selviytyjiin ja häviäjiin. Sanotaan, että kun organisaation jatkuvuus on uhattuna, ollaan usein jo kriisissä. Kriisit aiheuttavat aina organisaatioille toimintahäiriöitä, taloudellisia vahinkoja ja pitkittyessään usein myös mainehaittaa. (Finnish Information Security Cluster 2022, Artikkeli) Digitaalisessa maailmassa kyberturvallisuus ja sen hallinta on keskeinen elementti organisaation tavoitteiden toteuttamisessa. Asianmukainen kyberturvallisuuden hallinta edellyttää organisaatiolta johtoa myöten myönteistä kyberturvallisuuskulttuuria ja tarvittavia investointeja sen toteuttamiseen.

Finnish Information Security Clusterin (FISC) verkkoartikkelissa kuvataan, miten liiketoiminnan jatkuvuudenhallinta on viime vuosina priorisoitu yhä useammassa yrityksessä tärkeimpien asioiden listalle. Organisaatioiden operatiivinen toiminta edellyttää kasvavassa määrin digitaalisia tuotteita ja palvelualustoja. Viimeistään COVID-19:n aiheuttaman kriisin kautta useat organisaatiot ovat joutuneet digitalisoitumaan pakosta ja tällöin työntekijät ja heidän tietoturvallisuus osaamisensa on keskeinen osa kyberturvallisuutta ja sen onnistunutta hallintaa. Kyberuhkiin varautuminen on olennainen osa organisaation liiketoiminnan jatkuvuudenhallintaa ja toiminnan tulevaisuuden turvaamista. (Finnish Information Security Cluster 2022, Artikkeli)

Toiminnan jatkuvuuden varmistaminen on organisaation hallitusten vastuulla ja PwC:n artikkelin mukaan hallituksen tulisikin kyberturvallisuuteen liittyen kysyä säännöllisesti ylimmältä johdolta?

- Onko organisaatiolla tilannekuva sen kyberturvallisuuden tilasta?
- Miten sen kyberturvallisuutta johdetaan ja hallitaan?
- Onko kriittiset toimitusketjut ja niiden riskit tunnistettu?
- Onko se luotettava toimija sidosryhmien mielestä?
- Toimiiko organisaatio viranomaisvaatimusten mukaisesti?
- Harjoittelemmeko säännöllisesti kyberhyökkäystilanteiden hallintaa?
- Hyödynnämmekö kyberturvallisuustyötä liiketoimintamahdollisuuksien kasvattamisessa?

(PwC 2022, Artikkeli)

4.2 Varautuminen on ennakointia

Varautuminen tarkoittaa toimintaa, jolla varmistetaan palveluiden mahdollisimman häiriötön toiminta häiriötilanteissa eli turvataan toiminnan jatkuvuus. Tällaisia toimenpiteitä ovat esimerkiksi varautumissuunnittelu, ennakoivat toimenpiteet sekä kyberturvallisuus koulutukset ja harjoitukset. Varautuminen perustuu riskien arviointiin ja siinä on huomioitava uhkamallit. Uhkamalleja tarkennetaan ja päivitetään uhka-arvioiden muutosten perusteella säännöllisesti. (Turvallisuuskomitea 2022, Artikkeli)

Kuvan 18 mukaisesti varautumisessa pyritään reagoinnin sijasta ennakointiin. Ennakointi edellyttää suunnittelua ja toimenpiteitä suunnitelman perusteella. Keskeistä varautumisen kehittämisessä on myös eri tahoilta saatu palaute toimenpiteiden toimivuudesta.

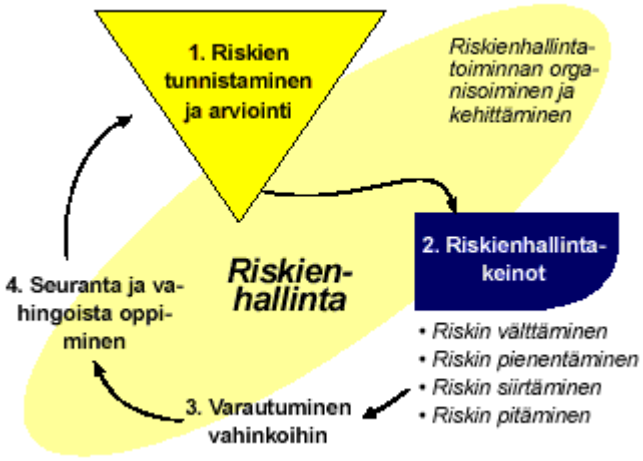
Kuva 18. Ennakointi ja varautuminen (Turvallisuuskomitea 2022 1, Artikkeli)

Kyberturvallisuusuhkien torjuminen edellyttää toimenpiteitä, jotka eivät onnistu pelkästään teknologian avulla. Keskeistä on henkilöstön kyberosaaminen sekä hallintaan liittyvät toimintamallit ja prosessit. (Cinia 2022, Artikkeli) Organisaation jatkuvuuden hallinta- ja häiriönsietokyky kehittyvät harjoittelemalla. Dokumentoitu varautumissuunnitelma ei varmista sitä, että organisaatio kykenisi toimimaan oikein organisaation toiminnan jatkuvuuden turvaamiseksi. Kriisi- ja häiriötilanteisiin harjoittelulla henkilöstö sitoutetaan organisaatiolle luotuihin jatkuvuussuunnitelmiin ja korostetaan ennalta sovittuja toimintatapoja. Tämä selkeyttää myös kriisin aikaisia rooleja sekä vastuita ja mahdollistaa oikeassa tilanteessa sujuvamman tilannejohtamisen. Harjoitukset ovat myös hyvä keino testata organisaation jatkuvuussuunnitelmaa, koska se paljastaa sen vahvuudet ja heikkoudet. (Finnish Information Security Cluster 2022, Artikkeli)

4.3 Riskienhallintaprosessi

Kyberturvallisuuden hallinnan tärkein prosessi on oikein toteutettu riskienhallinta. Se on erinomainen työväline, kun organisaation kehittää turvallisuuttaan lisääviä prosesseja, toimenpiteitä ja palveluita. Riskienhallinta lisää organisaation kustannustehokkuutta, kun kehitystoimenpiteet voidaan aidosti ohjata merkityksellisten asioiden korjaamiseen, joilla on laaja vaikutus tunnistetun uhkan todennä-

köisyyden tai vaikuttavuuden pienentämiseen. (Valtiovarainministeriön julkaisuja 22/2017, 5) Kyberturvaan liittyvät hallintatoimenpiteet eivät tule koskaan täysin valmiiksi. Uusia ongelmia tulee vastaan joka tapauksessa, joten organisaation on tärkeää ymmärtää riskienhallinnan perusperiaatteet.



Kuva 19. Riskienhallinnan prosessi (VTT 2009, Artikkeli)

4.3.1 Riskien tunnistaminen ja arviointi

Riskien tunnistamista ja arviointia suoritetaan yleensä organisaation jokaisella tasoilla; operatiivisella tasolla tunnistetaan käytännönläheiset ja toimintaan vaikuttavat riskit, kun taas yritysjohdon vastuulla on tunnistaa liiketoimintaa ja sen menestymistä uhkaavat tekijät. Organisaation riskejä voidaan tunnistaa useasta eri näkökulmista liittyen esimerkiksi ihmisiin, tietojärjestelmiin tai sidosryhmiin. Kun organisaation kaikki riskit yhdistetään samaan riskirekisteriin, voidaan sen avulla seurata organisaation riskitasoa kokonaisuudessaan, riskienhallintaan liittyviä toimenpiteitä sekä niiden vaikuttavuutta.

Kun kaikki yllä mainitut riskit on tunnistettu, tulee arvioida niiden kunkin osalta toteutumisen todennäköisyyttä ja vaikutuksia. Tämän perusteella valitaan kaikkein kriittisimmät riskit ja niiden hallitsemiseen kohdistetaan kaikki käytettävissä olevat organisaation resurssit.

Riskien realisoitumisen vaikutuksia tulee myös arvioida eri näkökulmista. Tyypillisesti riskin toteutuminen vaikuttaa negatiivisesti organisaation maineelle, operatiiviselle toiminnalle ja palvelujen saatavuudelle (esim. lakisääteisten tehtävien hoitaminen), sidosryhmille tai taloudelle.

4.3.2 Riskien hallintakeinot

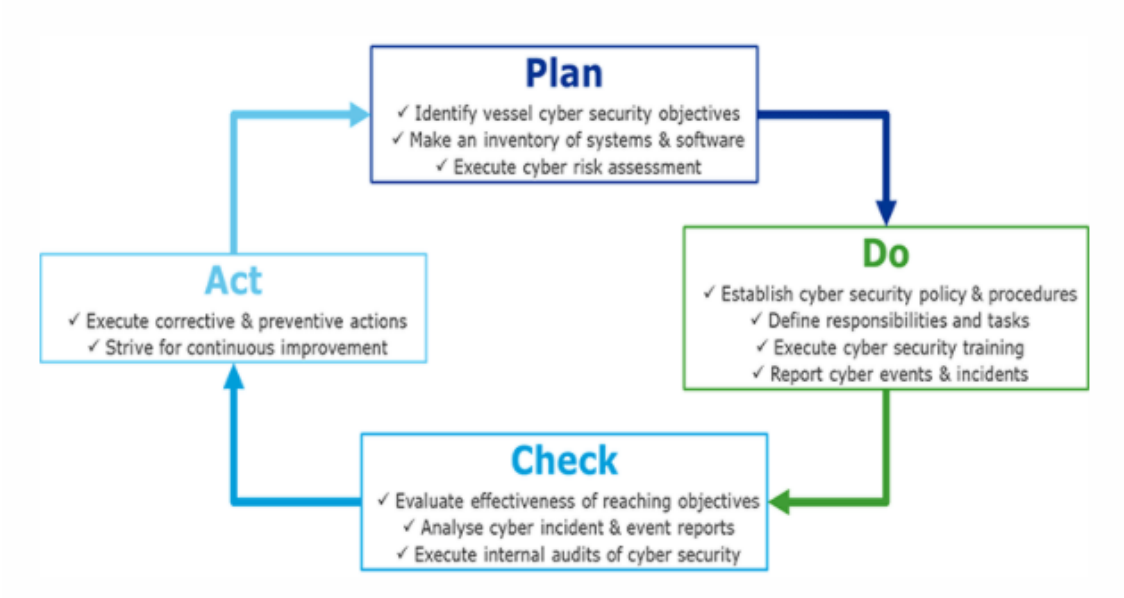
Riskien vähentämiseen tähtäävät hallintatoimenpiteet kohdistetaan ensisijaisesti kriittisimpiin riskeihin. Toimenpiteiden tavoitteena on alentaa riskin toteutumisen todennäköisyyttä tai vähentää riskin realisoitumisen vaikuttavuutta.

Kyberturvallisuuskeskus listaa riskinhallinnassa neljä yleistä mekanismia, joita voidaan tarpeen tullen yhdistellä riskinhallinnassa:

- Riskin välttäminen, eli riskin aiheuttava tekijä korjataan esimerkiksi paikkaamalla löydetty haavoittuvuus tai poistamalla riskin aiheuttava palvelu käytöstä.
- Riskin pienentäminen jollain tavalla, esimerkiksi rajaamalla pääsyä palveluun vain organisaation IP-verkkoalueesta, jolloin palvelun hyväksikäytön riski alenee, mutta se ei häviä kokonaan.
- Riskin siirtäminen jollain keinolla, esimerkiksi lisäämällä valvontaa riskin havaitsemiseen ja reagointikykyä riskin poistamiseen, jos se realisoituisi.
- Riskin pitäminen. Kun organisaation johdolle on kerrottu olemassa olevasta ongelmasta, sen vaikutuksista ja korjaavien toimien kustannuksista, päätetään ettei asialle tarvitse tehdä mitään. (Traficom 2019, Artikkeli)

4.3.3 Riskien seuranta ja vahingosta oppiminen

Digitaalisen toimintaympäristön muutokset ovat nopeita ja jatkuvia. Tästä syystä kyberturvallisuuden hallintamalliakin kehitetään jatkuvasti, jotta muutosten vaikutuksia organisaation toimintaympäristöön voidaan helpommin hallita. Jatkuvaa parantamista toteutetaan tyypillisesti PDCA-mallin (Plan-Do-Check-Act) avulla. Kuvassa 20. on esimerkinomaisesti esitetty hallintamallin luominen PDCA-prosessin avulla.



Kuva 20. Esimerkki PDCA-prosessista (DNV 2022, Artikkeli)

Suunnitteluvaiheessa (Plan) hallintamallille määritetään tavoitteet. Toteutusvaiheessa (Do) suoritetaan suunnitellut toimenpiteet haluttujen päämäärien saavuttamiseksi. Seurantavaiheessa (Check) yhdistetään hallintamallin toiminnasta saadut seuranta- ja mittaustiedot ja verrataan niitä asetettuihin tavoitteisiin. Kehittämisvaiheessa (Act) arvioidaan hallintamallin suorituskykyä ja mahdollisia poikkeamia ja näiden perusteella asetetaan uusia tavoitteita seuraavalle päivityskierrokselle.

Hallintamallin jatkuvan parantamisen tarkoituksena on ylläpitää se ajan tasalla toimintaympäristön muutoksissa. Toteutus sidotaan yleensä organisaation kehittämisen vuosikelloon ja kunkin kehitettävän asian toteutuksen sykli määritetään tehtävän, muutosnopeuden tai laajuuden mukaisesti.

4.4 Kyberturvallisuus tarvitsee johtamista

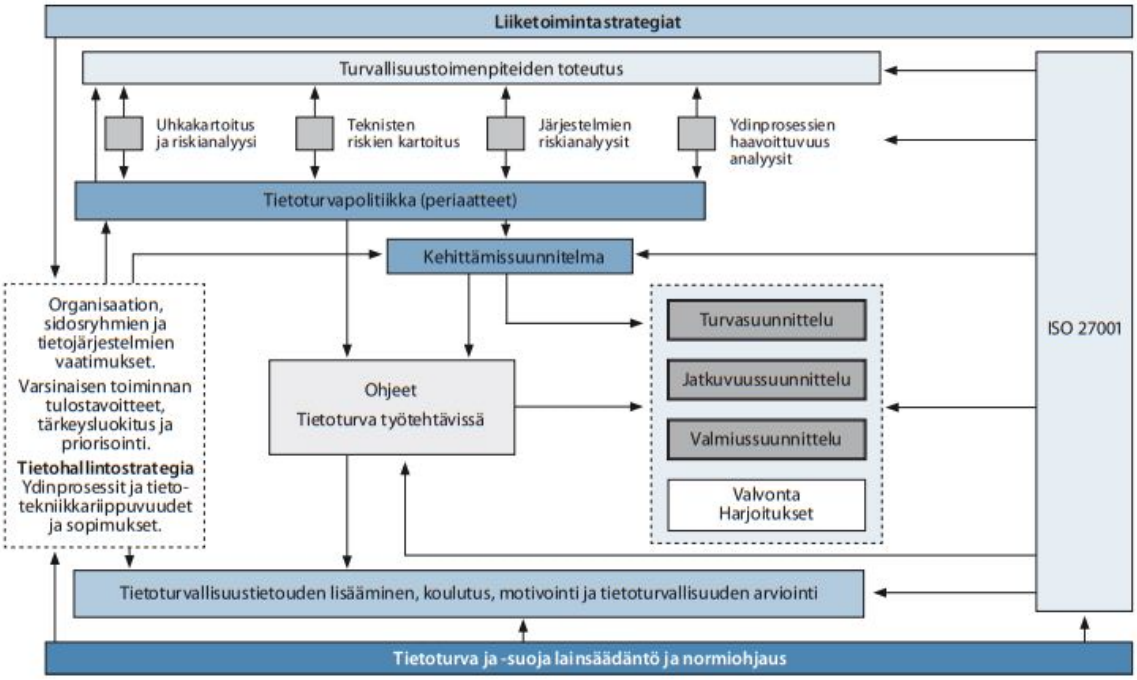
Kyberturvallisuudesta vastuu on aina organisaation toimivalla johdolla. Kyberturvallisuutta kehitettäessä organisaation johdon on päätettävä toimintatapa, jolla organisaation kyberturvallisuuteen liittyvät riskit saadaan hallintaan. Kyberturvallisuusstrategia on ensimmäinen asia, joka johdon tulee laatia. Sen tehtävä on antaa korkean tason ohjeet, joista tekniset asiantuntijat sitten soveltavat yksityiskohtaiset toimintaohjeet. (Limnell ym. 2014, 157–158, 171.) Henkilöstö on usein kyberturvallisuuden heikoin kohta inhimillisten virheiden kautta. Selkeät ja henkilöstölle läpikäydyt turvallisuusohjeet parantavat jokaisen työntekijän päivittäistä toimintaa ja tahalliset hyökkäykset voidaan usein estää jo sillä, että suojattavaa tietoa käsitellään turvallisemmin. (Teknologiateollisuus 2021, Artikkeli)

Johdon luoma kyberturvallisuusstrategia toimii organisaation kyberturvallisuusohjelman perustana ja siinä määritetään kyberturvallisuusohjelman hallintamalli ja valvontatoimenpiteet. Yksinkertaisimmassa muodossa kyberturvallisuusstrategia voi sisältää listan organisaation kyberturvallisuustavoitteita ja suunnitelman niiden toteuttamisesta. Organisaation kyberturvallisuuskypsyyden kasvaessa organisaation ylemmän johdon osallistuminen kyberturvallisuusohjelman suunnitteluun vahvistuu ja näin myös kyberturvallisuusstrategiasta tulee kattavampi sisällön osalta. (Traficom 2020 4, Artikkeli)

4.5 Kyberturvallisuuden johtamis- ja hallintamalli

Organisaation kyberturvallisuusohjelman toteuttamisessa kannattaa hyödyntää standardeihin perustuvia hallintajärjestelmiä. Niissä on määritelty hyväksi todetut tieto- ja kyberturvallisuuden johtamisessa, hallinnoimisessa ja valvonnassa vaadittavat menettelyt ja toimenpiteet. Tällainen hallintamalli ei ole yksittäinen dokumentti, vaan laaja-alainen prosessi, jota tulee kehittää jatkuvasti ja kokonaisuutena sen luominen on monivuotinen projekti.

Hallintamalli määrittää organisaatiolle selkeästi kaikkien tiedossa olevat kyberturvallisuuden hallintatavoitteet. Ne voidaan kuvata esimerkiksi tietoturvapolitiikassa, jatkuvuussuunnitelmassa tai muussa soveltuvassa asiakirjassa. (Digi- ja väestötietovirasto 2021, 6) Kuvassa 21 on kuvattu esimerkinomaisesti tietoturvallisuuden hallintamallin perusrakenne.



Kuva 21. Tietoturvallisuuden hallintamallin malliesimerkki (Valtiovarainministeriö 2007, 41)

Hallintamalli tähtää organisaation tavoitteiden saavuttamiseen käytössä olevien resurssien puitteissa. Hallintamalli sisältää organisaatiorakenteen, politiikat, suunnittelutoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit ja resurssit. Se muodostuu selkeistä toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista ja toiminnoista, joita organisaatio hallinnoi kokonaisuutena suojatakseen sen tieto-omaisuutta. Hallintamalli perustuu organisaation toimintastrategiaan sekä kokonaisvaltaiseen riskienhallinnan suunnitteluun. Alla listattu keskeiset hallintamallin sisältämät toimintamallit ja dokumentit: (Valtionvarainministeriö 2006, 19)

Tietoturvallisuuden hallintamalli on luonteeltaan viitekehys, joka koostuu mm. seuraavista toimintamalleista ja dokumenteista: (Valtiovarainministeriö 2007, 40)

- Tietoturvapolitiikka ja -strategia
- Tietoturvakäytännöt ja -periaatteet
- Tietoturvallisuuden kehittämissuunnitelma
- Tietoturvallisuuden perus- ja lisäohjeistus
- Tietoturva-arkkitehtuurit
- Tietoturvaraportointi johdolle
- Jatkuvuus- ja valmiussuunnitelmat
- Toimintaan liittyvät tietoturvaprosessit
- Auditointisuunnitelma.

Hallintamallin käyttö helpottaa organisaation mahdollisuuksia täyttää asiakkaiden ja sidosryhmien kyberturvavaatimukset määräysten ja sopimusten mukaisesti. Se parantaa myös organisaation suunnitelmia ja toimintatapoja toteuttaa määritettyjä kyberturvatavoitteita hallitulla ja johdonmukaisella

tavalla. Kun organisaatio ottaa käyttöön kyberturvallisuuden hallintamallin, se voi osoittaa myös sidosryhmilleen kykynsä noudattaa molempien osapuolia tukevia kyberturvaperiaatteita. (SFS-EN ISO 27000:2020 16–23)

Toimiva kyberturvallisuuden hallintamalli suojaa niin tieto-omaisuutta kuin antaa organisaatiolle mahdollisuuden saavuttaa entistä parempi varmuus siitä, että sen tieto-omaisuus on jatkuvasti suojattu riittävän hyvin uhkilta. Se myös ylläpitää määrämuotoista toimintatapaa, jonka avulla voidaan tunnistaa ja arvioida kyberriskit, valita ja toteuttaa soveltuvat hallintakeinot sekä mitata ja parantaa toimenpiteiden vaikuttavuutta. (SFS-EN ISO 27000:2020 16–23)

Kyberturvallisuuden hallintamallia luotaessa organisaation käy tyypillisesti läpi seuraavat hyväksi havaitut toimenpiteet, joilla se kykenee luomaan hallintamallin sekä seuraamaan, ylläpitämään ja parantamaan sitä jatkossa:

1. Tunnistetaan organisaation toimintaympäristö (organisaation tehtävä, sidosryhmät)
2. Määritetään organisaation tavoitteet ylätasolla (strategiset linjaukset)
3. Arvioidaan organisaation kyberturvallisuus riskit ja niiden vaikutukset (riskien arviointi ja vaikutusanalyysi)
4. Kohdistetaan organisaation resurssit riskiarvion ja asetettujen tavoitteiden mukaisesti (hallintatavoitteet)
5. Määritellään hallintatoimenpiteet, joilla tavoitteisiin on tarkoitus päästä ja varmista tulokset (hallintakeinojen mittaus ja seuranta)
6. Kehitetään hallintamallia saatujen havaintojen perusteella (jatkuva parantaminen) (Digi- ja väestötietovirasto 2021, 6)

Jotta hallintamallin suojaavuus uusi uhkia tai muuttuvaa ympäristöä vastaa voidaan varmistaa, täytyy riskien, organisaation strategioiden tai liiketoimintatavoitteiden muutokset tunnistettava ja arvioitava jatkuvasti toistamalla listan vaiheita 1–6. Esimerkiksi ISO 27001 standardi edellyttää, että organisaation tietoturvapolitiikassa käytetään jatkuvaan parantamisen menetelmiä hallintamallin tukena. (ICT Institute 2017, Artikkeli)

4.6 NIST-kyberturvallisuuden viitekehys

Kyberturvallisuuden hallintamallin kehittämisen tueksi löytyy useita hyväksi havaittuja viitekehyksiä, jotka auttavat keskittymään oleellisiin ja käytännössä hyväksi todettuihin kyberturvaa parantaviin asiakokonaisuuksiin. Seuraavassa on esitelty vuonna 2014 julkaistu National Institute of Standards and Technologyn (NIST) kyberturvallisuuden viitekehys (CSF). Se luotiin aikanaan USA:n presidentin määräyksestä kriittisen infrastruktuurin suojaamiseksi. Viitekehys ei korvaa organisaation olemassa olevia prosesseja, mutta se tarjoaa yhteisen kielen kyberturvallisuusriskien ymmärtämiseen, hallintaan ja kommunikointiin niin organisaation sisäisille kuin ulkoisille sidosryhmille. (NIST 2018, 13) Suomen Kyberturvallisuuskeskuksen kyberturvallisuuden arviointityökalu Kybermittari pohjautuu vahvasti NIST-viitekehykseen. (Traficom 2020 2, 4)

4.6.1 Viitekehyksen rakenne

NIST-viitekehys rakentuu kuvan 18 mukaisesti neljästä osa-alueesta: toiminnot (Funktiot), kategoriat (Categories), alakategoriat (Subcategories) ja viittaukset (Informative References). (NIST 2018, 6–7)

Kuva 22. NIST Framework Core (NIST 2018, 6-7)

Toiminnot (Functions)

NIST-viitehys on jaettu viiteen toimintoon: tunnistaminen (Identify), suojautuminen (Protect), havainnointi (Detect), reagointi (Respond) ja palautuminen (Recover). Toiminnot ovat rinnakkaisia ja ne edustavat kyberturvallisuuden elinkaarta. Jokainen toiminto on tärkeä ja välttämätön osa kyberriskien hallinnan kannalta. (NIST 2018, 7–8.)

Kyberturvallisuuden hallinnan kannalta ensimmäinen ja tärkein vaihe on tunnistaa organisaation toiminnot, prosessit ja tietojärjestelmät. Riskienhallinnan kautta arvioidaan niiden kriittisyys ja suojaustarpeet. Kun tunnistus on tehty, tehdään sen perusteella tarvittavia suojaustoimenpiteitä. Kun kriittisten toimintojen suojaukset ovat kunnossa, voidaan havainnoida niiden toimintaa ja tarvittaessa kehittää suojausta lisää. Mikäli kyberuhkatilanne tapahtuu, tulee se havaita ajoissa ja siihen tulee pystyä reagoimaan. Palautuminen pitää sisällään häiriöstä oppimisprosessin (Lessons learned). Sen tarkoituksena on varmistaa, että haavoittuvuus on korjattu, prosessit ovat toimintakuntoisia ja tapahtumasta on opittu. (NIST 2018, 7–8.)

Kategoriat (Category) ja alakategoriat (Subcategory)

Viitekehyksen toiminnoilla on 21 kategoriaa ja yli 100 alakategoriaa. Alakategoriat tarjoavat kullekin kategorialle kontekstin viitaten toisiin viitekehyksiin, kuten esimerkiksi COBIT- ja ISO-standardit. Alla esimerkki tunnista toiminnon yhdestä kategoriasta ja sen alakategorioista ja viitteistä. (NIST 2018, 7–8.)

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Kuva 23. Framework core (NIST 2018 1)

Kunkin NIST-viitekehyksen toiminnon kategoriat ovat seuraavat:

4.6.2 Kyberturvallisuusympäristön ja riskien tunnistaminen (Identify)

Tunnistamistoiminnon tavoitteena on auttaa organisaatiota määrittää kyberturvallisuusohjelman perusta. Organisaation on ymmärrettävä nykyinen liiketoimintaympäristönsä varmistaakseen, että se voi hallita organisaation tietoihin, järjestelmiin ja omaisuuteen kohdistuvia kyberturvallisuusuhkia. Organisaation tulee inventoida ja arvioida omaisuuttaan ja miten eri osat liittyvät toisiinsa ja mitkä vastuut tai roolit työntekijöillä on niiden johtamisessa.

Tunnista toiminnon kategoriat ovat: (NIST 2018, 24–29):

- Liiketoimintaympäristö (Business Environment) – Organisaation tulee tunnistaa oma roolinsa toimitusketjussa ja määrittää organisaation missio, tavoitteet, yleiset toiminnot ja sidosryhmät. Nämä tiedot tulee sitten priorisoida ja käyttää kyberturvallisuusroolien ja -vastuiden jakamiseen sekä riskienhallintapäätösten tekemiseen.
- Omaisuudenhallinta (Asset Management) – Organisaation tulee tunnistaa kaikki kyberturvallisuusresurssit eli laitteet, tiedot, henkilötiedot, tilat ja järjestelmät, joiden avulla se voi saavuttaa liiketoimintatarkoituksensa. Nämä tunnistetut omaisuuserät olisi tunnistettava ja hallittava sen perusteella, miten tärkeitä ne ovat liiketoimintatavoitteisiin nähden ja millaisia kyberturvallisuusriskejä organisaatio pitää hyväksyttävinä tai ei -hyväksyttävinä niiden osalta.

- Hallinto (Governance) – Organisaation tulee luoda menettelyt, prosessit ja politiikat, jotka ovat tarpeen yrityksen riskien, oikeudellisten, toiminnallisten ja sääntelytarpeiden hallitsemiseksi ja valvomiseksi. Niitä tulee käyttää sitten kyberturvallisuusriskien hallintaa koskevien päätösten tekemiseen.
- Riskinarviointi (Risk Assessment) – Organisaation tulee ymmärtää kyberturvallisuusriskit, joita sen omaisuus, toiminta ja työntekijät voivat kohdata ja käyttää näitä uhkia, haavoittuvuuksia, niiden esiintymisen todennäköisyyttä ja liiketoiminnallisia vaikutuksia riskien määrittämisessä.
- Riskienhallintasuunnitelma (Risk Management Strategy) – Organisaation tulee määrittää sen riskiensietokyky, prioriteetit ja rajoitukset ja käyttää näitä tietoja kriittisten kyberturvallisuusriskejä koskevien operatiivisten päätösten tukena.

Kaikki NIST-viitekehyksen toiminnot ovat tärkeitä eri syistä mutta tämä tunnistamistoiminto (Identify) on perustavanlaatuinen. Siinä on kyse organisaation omaisuuden ja sen kriittisyyden ymmärtämisestä, eli niistä asioista, joihin kyberturvariskit voivat kohdistua ja mihin muiden viitekehyksen osioiden toimenpiteillä yritetään vaikuttaa riskien pienentämiseksi tai estämiseksi. (Balbix 2022, Artikkeli)

4.6.3 Kyberhäiriötilanteilta suojautuminen (Protect)

Kun organisaatio ymmärtää kyberturvariskinsä, se voi arvioida, tarjoavatko sen olemassa olevat kyberturvallisuustoimenpiteet riittävän suojan vai tarvitaanko lisätoimenpiteitä palvelujen toimittamisen varmistamiseksi. Suojautumistoiminto määrittää suojatoimenpiteitä kriittisen infrastruktuurin palveluiden toiminnan varmistamiseksi ja se tukee kykyä rajoittaa ja hillitä mahdollisen kyberturvallisuusuhkan vaikutuksia.

Suojautumistoiminnon alakategoriat ovat: (NIST 2018, 29–37):

- Identiteetin hallinta ja käytönvalvonta (Access Control) – Organisaatio rajoittaa pääsyä verkkoon ja omaisuuteen varmistaaksesi, että käyttäjillä on mahdollisimman vähän käyttöoikeuksia, joita he tarvitsevat työtehtäviensä hoitamiseen.
- Koulutus ja tietoisuus (Avareness and Training) – Organisaatio tarjoaa riittävästi koulutusta ja kyberturvallisuustietoisuutta, jotta työntekijät voivat suorittaa velvollisuutensa yrityksesi tietoturvakäytäntöjen ja -menettelyjen mukaisesti.
- Tietoturva (Data Security) – Organisaatio hallitsee kriittisiä tietoja riskinarviointistrategiansa perusteella, joka on suunniteltu turvaamaan kriittisten tietojen luottamuksellisuus, saatavuus ja eheys.
- Tietosuojamenettelyt ja -prosessit (Info Protection Processes and Procedures) – Organisaatiolla on prosessit, politiikat ja menetelmät, joita käytetään sen tietojärjestelmien ja omaisuuden tehokkaaseen suojaamiseen. Tällaisia ovat esimerkiksi peruskonfiguraatio (palvelujen perusasetukset, mihin ne voi turvallisesti palauttaa häiriön jälkeeni), elinkaarenhallinta, muutoshallinta, varmistus, reagointi- ja jatkuvuussuunnitelmat.

- Ylläpito (Maintenance) – Organisaatiolla on mekanismit tietojärjestelmien korjauksiin, jotta ne tehdään yrityksen hyvien toimintatapojen ja käytäntöjen mukaisesti. Eli omaisuuden huoltoa suoritetaan tavalla, joka estää sen luvattoman käytön.
- Suojaustekniikka (Protective Technology) – Organisaatiolla on automaattisia ja manuaalisia toimintoja ja työkaluja tietoturvasta huolehtimiseen. Esimerkiksi lokitiedot, siirrettävät tietovälineet ja noudatetaan vähimmän toiminnallisuuden periaatetta.

4.6.4 Kyberhäiriötilanteen havaitseminen (Detect)

Kyberuhkien lieventämisessä nopeus on ratkaisevan tärkeää, joten välitön kyberhäiriöiden havaitseminen on oleellista, koska se mahdollistaa oikea-aikaiset vastatoimenpiteet. Tämä havaitsemistoiminto määrittää tarvittavat toimenpiteet kyberturvallisuusuhkan havaitsemiseksi ajoissa.

Havaitse toiminnon alakategoriat ovat: (NIST 2018, 37–40):

- Poikkeavuuksien havaitseminen (Anomalies and Events) – Organisaation on varmistettava, että kaikki kybertapahtumat tai -poikkeamat havaitaan nopeasti.
- Jatkuva seuranta (Securitys Continuous Monitoring) – Organisaation tulee seurata tietoja ja omaisuutta jatkuvasti, jotta se havaitsee nopeasti kyberturvallisuustapahtumat.
- Havaintoprosessit (Detection Processes) – Organisaation tulee ylläpitää tunnistusprosesseja varmistaakseen niiden saatavuuden ja luotettavuuden mahdollisten poikkeamien havaitsemiseksi.

4.6.5 Kyberhäiriötilanteeseen reagointi (Respond)

Mitä tapahtuu, jos kyberriskit toteutuvat ja organisaation järjestelmiin murtaudutaan? Organisaatiolla tulee olla käytössä etukäteen suunnitellut turvallisuuspoikkeamien hallintatoimenpiteet hyökkäysten vaikutusten minimoimiseksi. Reagointitoiminto keskittyy toimenpiteisiin havaitun kyberturvallisuushäiriön sattuessa ja tukee kykyä hillitä mahdollisen kyberturvallisuushäiriön vaikutuksia.

Reagointi toiminnon alakategoriat ovat: (NIST 2018, 41–43):

- Reagoinnin suunnittelu (Response Planning) – Varmistaa oikea-aikainen reagointi käyttämällä oikein suoritettuja toimenpiteitä ja prosesseja.
- Viestintä (Communication) – Kattaa ulkoisten ja sisäisten sidosryhmien väliseen viestintään liittyvät vastatoimet
- Analyysi (Analysis) – Sisältää tarkastelut, jotka on tehty vastatoimien aikana varmistaakseen, että oikeita menettelyjä noudatetaan
- Riskien vähentäminen (Mitigation) – Kattaa toimet, jotka estävät kyberturvallisuustapahtuman laajenemisen muihin järjestelmiin tai muihin verkon osiin.
- Parannukset (Improvements) – Joka kerta, kun organisaatio tekee vastatoimia, se tarjoaa uusia mahdollisuuksia prosessin parantamiseen tarkastelemalla opittuja asioita ja tekemällä parannuksia.

4.6.6 Kyberhäiriötilanteesta palautuminen (Recover)

Palautumistoiminto sisältää toimenpiteet, joilla ylläpidetään jatkuvuussuunnitelmia ja palautetaan kyberturvallisuushäiriön vuoksi heikentyneet ominaisuudet tai palvelut. Oikea-aikaiset toimenpiteet normaali toimintaan palautumisessa vähentävät kyberturvallisuushäiriön vaikutusta. Palautumistoiminnon toimenpiteet ovat osittain päällekkäisiä reagointitoimien kanssa.

Palautumistoiminnon alakategoriat ovat: (NIST 2018, 43–44):

- Palautumisen suunnittelu (Recovery Planning) – Toipumismenettelyjen järjestäminen tärkeysjärjestyksen perusteella.
- Parannukset (Improvements) – Parannetaan toipumissuunnitelmaa ja -prosesseja sisällyttämällä saadut kokemukset tulevaan toimintaan.
- Viestintä (Communication) – Yhteydenpidon koordinointi kaikkien sidosryhmien kanssa palvelujen onnistuneen palauttamisen varmistamiseksi.

4.7 Työkaluja hallintamallin kehittämiseen

Kyberturvallisuuden hallintamalli luomiseen löytyy edellä kuvatun NIST-viitekehyksen lisäksi lukuisia viranomaisten, järjestöjen ja yksilöiden laatimia julkaisuja, joissa käsitellään kyberympäristön tietoturvahaasteisiin vastaamista. (Keskuskauppakamari 2021, 6)

Alla luettelo tunnetuimmista kyberturvallisuus julkaisusta lueteltuna yleisestä yksityiskohtaiseen:

- Suositukset ovat ylätason visioita, jotka määrittävät tietoturvan huolenaiheita ja suuntaviivoja organisaatioille. Esimerkiksi OECD Security Guidelines.
- Kansalliset strategiat ovat suosituksia, joissa kuvataan kansalliseen tai lainsäädäntöön sovellettu tapa hoitaa kyberturvallisuutta. Esimerkiksi International Strategy to Secure Cyberspace, Euroopan ja muiden maiden kansalliset strategiat jne.
- Viitekehykset kokoavat yhteen kansallisista strategioista hyväksi todettuja aineistoja, joiden avulla organisaatiot voivat vertailla kehitystasoaan ja edistymistään tietoturvariskien käsittelyssä. Esimerkiksi NIST Cybersecurity Framework.
- Standardit ovat organisaation prosesseja sääteleviä vaatimuksia, joilla varmistetaan tietoturvan parhaiden käytäntöjen määrätietoinen ja johdonmukainen noudattaminen. Esimerkiksi ISO 27001, 27002 ja 27032-prosessistandardit ja kansainväliset maksukorttialan tietoturvastandardit.
- Tekniset standardit ovat tietyn rajapinnan toteutuksen yksityiskohtainen tekninen määrittely.

Suomessa kansallisella tasolla erinomaisia työkaluja kyberturvallisuuden parantamiseen ovat Katakri – tietoturvallisuuden auditointityökalu viranomaisille ja Vahti -ohjeet. Kyberturvallisuuskeskus julkaisee myös Kybermittaria, jolla organisaatio voi arvioida omaa kyberturvallisuuskyvykkyyttään.

4.7.1 ISO/IEC 27000 -standardi

”ISO 27001 -standardi määrittää tietoturvallisuuden hallintamallin luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevia vaatimuksia.” (SFS-EN ISO 27000:2020)

Näiden standardin määrittämien vaatimusten tavoitteena on suojata organisaation tiedon luottamuksellisuutta, eheyttä ja saatavuutta prosessien, ohjeiden, riskienhallinnan ja -hallintakeinojen avulla.

Standardi sisältää seitsemän pakollista vaatimusta, jotka organisaation tulee täyttää. Vaatimukset käsittelevät organisaation toimintaympäristöä, johtajuutta, suunnittelua, tukitoimintoja, itse toimintaa, suorituskyvyn arviointia ja jatkuvaa parantamista.

Velvoittavien vaatimusten lisäksi standardi määrittelee 114 valinnaista hallintakeinoa, joista riskianalyysin perusteella organisaatio voi valitaan tarpeelliset hallintakeinot toteutettavaksi.

<u>Hallintatavoitteet ja -keinot</u>

- ”Tietoturvapolitiikat
- Tietoturvallisuuden organisointi
- Henkilöstöturvallisuus
- Suojattavan omaisuuden hallinta
- Pääsynhallinta
- Salaus
- Fyysinen turvallisuus ja ympäristön turvallisuus
- Käyttöturvallisuus
- Viestintäturvallisuus
- Järjestelmien hankkiminen, kehittäminen ja ylläpito
- Suhteet toimittajiin
- Tietoturvahäiriöiden hallinta
- Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökulmia
- Vaatimustenmukaisuus” (SFS-EN ISO 27000:2020)

Kun organisaatio toimii standardin mukaisesti, kyseessä ei ole yksittäinen kehitysprojekti, vaan toimintatapa, joka näkyy organisaation päivittäisessä toiminnassa.

4.7.2 Katakri 2020

”Katakri 2020 on auditointityökalu, jota viranomainen voi käyttää arvioidessaan kohdeorganisaation kykyä suojata salassa pidettävää tietoa. Katakria voidaan hyödyntää arvioidessa yrityksen turvallisuusjärjestelyjä sekä viranomaisten tietojärjestelmien turvallisuutta.” (Traficom 2020 1)

”Katakrin avulla pyritään varmistamaan, että kohdeorganisaatiolla on riittävät turvallisuusjärjestelyt salassa pidettävien tietojen paljastumisen ehkäisemiseksi kaikissa niissä toimintaympäristöissä, joissa luottamuksellista tietoa käsitellään.” (Traficom 2020 1)

Katakriin on koottu sekä kansallisiin säädöksiin kuin kansainvälisiin velvoitteisiin perustuvat tietoturvallisuuden vähimmäisvaatimukset.

Katakri on jaettu kolmeen osa-alueeseen:

- ”Turvallisuusjohtamista koskevassa osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintamalli sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen.
- Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
- Teknistä tietoturvallisuutta koskevassa osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.” (Ulkoministeriö 2020, 5)

4.7.3 Vahti -ohjeet

VAHTI-vaatimusten hallintamalli 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. (Suomidigi 2021)

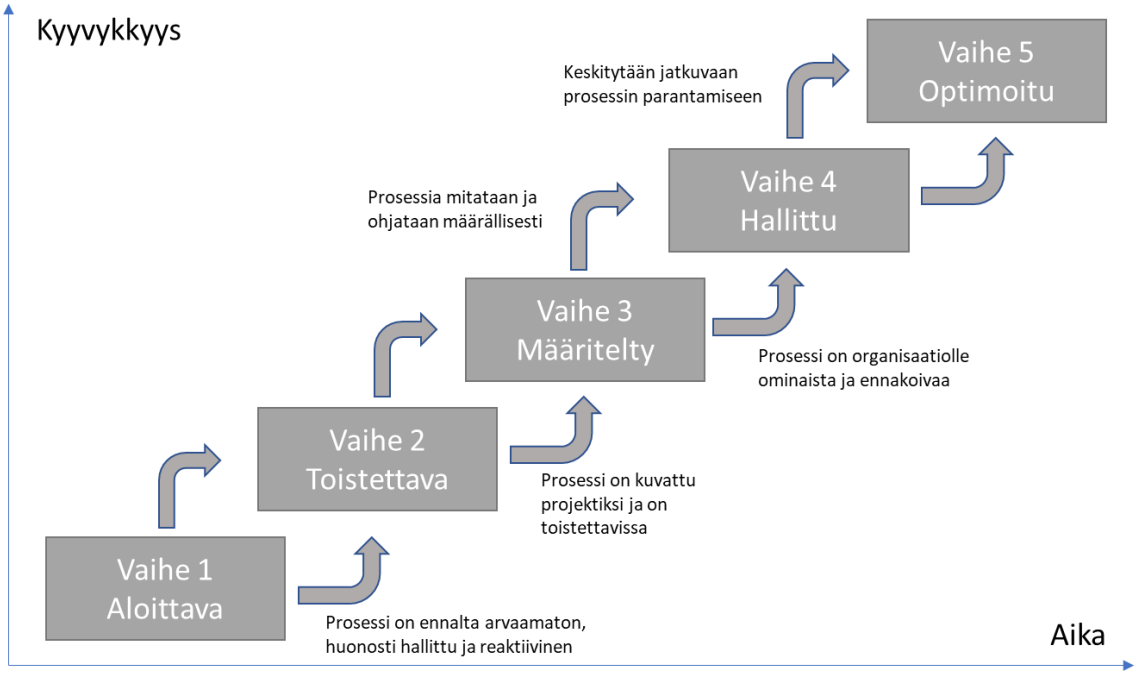
VAHTI-ohjeisto jakaa tietoturvallisuuden kahdeksaan osa-alueeseen.

- ”Hallinnollinen turvallisuus, johon sisältyvät johdon hyväksymät periaatteet, käytettävissä olevat resurssit, vastuunjako ja riskien arviointi.
- Henkilöstöturvallisuus, johon sisältyy henkilöstöön liittyvien luotettavuusriskien minimointi esimerkiksi toimenkuvien, käyttöoikeuksien määrittelyn, koulutuksen ja valvonnan sekä turvallisuusselvitysten avulla.
- Fyysinen turvallisuus, jolla tarkoitetaan laitteisto-, käyttö- ja arkistotilojen suojaamista fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä.
- Tietoliikenneturvallisuus, jolla tarkoitetaan tietoverkoissa liikkuvien tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseen liittyviä toimenpiteitä.
- Laitteistoturvallisuus, jolla tarkoitetaan tietojenkäsittely- ja tietoliikennelaitteiden turvallisuusominaisuuksia mukaan lukien yhtenäinen laitteistopolitiikka ja huoltosopimukset.
- Ohjelmistoturvallisuus, johon sisältyvät käyttöjärjestelmien, tietoliikenneohjelmistojen ja sovellusohjelmistojen turvallisuusominaisuudet.
- Tietoaineistoturvallisuus, jolla tarkoitetaan tietojen ja tietojärjestelmien tunnistamista ja luokittelua sekä tietovälineiden hallintaa ja säilytystä koko niiden elinkaaren ajan.
- Käyttöturvallisuus, jolla tarkoitetaan niitä menettelytapoja, joilla päivittäisessä toiminnassa säilytetään hyvä tietoturvallisuuden taso. Käyttöturvallisuus liittyy henkilöstön työkäytäntöjä

koskeviin periaatteisiin, tietojenkäsittelyn käyttöympäristöön ja turvallisuuteen liittyvien tapahtumien valvontaan.” (Suomidigi 2021)

4.8 Hallintamallin kehittäminen on evoluutioprosessi

Kun organisaation on valinnut toiminnalleen sopivan viitekehyksen kehitystoimenpiteiden tueksi, alkaa vasta varsinainen toiminnan kehitystyö. ”Hallintamallin kehittäminen on monivuotinen tehtävä, jossa organisaatiolle kehittyy valmiudet hallita järjestelmällisesti kyber- ja tietoturva-asioitaan. Hallintamallin kypsyysaste voidaan kuvata ja tämän toimintamallin tuloksena saadaan organisaation käyttöön tietoturvallisuuden tilan kuvaus ja voidaan tunnistaa siihen liittyvät kehittämistarpeet. Tietoturvallisuuden ja riskienhallinnan kehittäminen on jatkuva prosessi, jossa systemaattisesti pyritään edistämään organisaation laillisuuteen, tuloksellisuuteen, tieto-omaisuuden turvaamiseen ja tietoturvapoikkeamien luotettavaan raportointiin liittyviä tavoitteita.” (Valtiovarainministeriö 2006, 20)



Kuva 24. Kypsyysmalli (Capability Maturity Model) mukailtu (Harris, Maymi, 1111–1112)

Seuraavassa on esitetty lyhyet kokemusperäiset kuvaukset kustakin kehitysvaiheesta.

- Aloitusvaiheessa kyberturvatyö on vielä organisoitumatonta ja toimenpiteet reaktiivisia. Erilaisia ohjeita laaditaan, mutta ne ovat vielä hajanaisia ja kyberturvallisuuteen liittyvät vastuut puutteellisesti määriteltyjä. Organisaatio luo itselleen kyberturvapolitiikan sekä määrittää kyberturvallisuusvastuut.
- Toisessa kehitysvaiheessa keskistä on toimenpiteiden toistettavuus. Organisaatiossa on luotu kyberturvallisuuden hallintaan määrämuotoisia toimintatapoja. Sitä osoittavat esimerkiksi toteutettu kyberturvapolitiikka, myös käytössä oleva kyberturvallisuuden kehittämissuunnitelma. Kyberturvallisuuden järjestelmällinen kehittäminen on käynnistynyt.
- Kolmannessa vaiheessa organisaatiolle luodaan kyberturvallisuuden hallintamalli, jolloin kyberturvaprosessit ja päämäärät on määritelty. Kyberturvallisuuden ohjeistus on kattava,

henkilöstön kyberturvakoulutus on keskeinen osa toimintamallia ja organisaatio noudattaa suunniteltua kehittämissuunnitelmaa.

- Neljännessä vaiheessa toimitaan luodun kyberturvallisuuden hallintamallin mukaisesti. Toiminnalle on asetettu tuloksellisuuden ja kehittämistarpeiden määrittämistä varten mittaristo. Tässä vaiheessa voidaankin sanoa, että organisaatiolla on kyberturvallisuuden johtamis- ja hallintamalli olemassa.
- Viidennessä vaiheessa kyberturvallisuuden johtamis- ja hallintamallia optimoidaan esimerkiksi auditointien, toisilta organisaatioilta saatujen kokemusten ja muun oppimisen kautta. Turvallisuusasioiden on oltava kiinteä osa organisaation toimintakulttuuria, jotta niistä tulee jokapäiväinen ja luonteva osa organisaation toimintaa. (Valtiovarainministeriö 2006, 21–22)

5 KYBERTURVALLISUUDEN MITTAAMINEN

5.1 Kyberturvallisuuden vuositavoitteet

Organisaation strategisena tavoitteena on luoda sille kyberturvallisuuden johtamis- ja hallintamalli ja sen tavoitetaso määräytyy organisaation toiminnan luonteen ja riskien pohjalta. Tämän tavoitetason edellyttämän hallintamallin kehittäminen kestää tavallisesti vuosia ja tästä syystä kehittämistavoitteet tulee jaksottaa usealle vuodelle niin toiminta- kuin taloussuunnitelmassa. Hallintamallin kehittäminen kannattaa jakaa pienempiin kokonaisuuksiin ja aloittaa aivan perustasosta. Perustan muodostavat riskien arviointi, tietoturvapolitiikka, kehittämissuunnitelma sekä tarvittava ohjeistus ja koulutus. (Valtiovarainministeriö 2006, 25)

Vuositavoitteet voidaan jakaa kahteen osaan:

- Kyberturvallisuuden kehittämiseen liittyvät tavoitteet
- Tavoiteltavaan ja mitattavissa oleva kyberturvatasoon liittyvät tavoitteet. (Valtiovarainministeriö 2006, 25)

Kyberturvallisuuden kehittämistavoitteilla varmistetaan johtamis- ja hallintamallin kehittyminen haluttuun tavoitetasoon. Erotuksena kehitystehtävistä, voidaan operatiiviselle kyberturvallisuustoiminnalle asettaa kvantitatiivisilla eli määrällisillä mittareilla osoitettavia tuloksellisuus- ja laatutavoitteita. ”Tyypillisiä tavoitteita ovat esimerkiksi häiriöiden vähentyminen, koulutuksen toteutuminen, tietoturvatoiminnan kustannuksiin liittyvät tavoitteet tai pisteyttää toimintaa laadullisen arvioinnin näkökulmasta - arvioimalla esimerkiksi kypsyystasoa.” (Valtiovarainministeriö 2006, 26)

5.2 Arviointi- ja mittausmenetelmät

Keskeinen osa kyberturvallisuuden hallintamallin toimintaa ovat arvioinnit ja ne muodostavat osaltaan sille mittareita. Laadullisia menetelmiä ovat muun muassa erilaiset arviot ja raportoidut tapahtumat, kun taas määrälliset arviot perustuvat aina systemaattiseen mittaamiseen. Arviointi on luonteeltaan jatkuva toiminto ja sitä käytetään kyberturvallisuuden kehittämiseen ja laadun parantamiseen. (Valtiovarainministeriö 2006, 32)

Arviointeja tehdään myös ulkoisten sidosryhmien vaatimusten perusteella. (Valtiovarainministeriö 2006, 32)

- Itsearviointi on laadunhallinnan yhteydessä usein käytetty systemaattinen toiminnan kehittämismenetelmä ja se soveltuu hyvin tietoturvallisuuden kehittämismenetelmäksi osana hallintamallia. Tällaisia itsearviointeja ovat esimerkiksi Katakrin itseauditointi ja Kybermittarin kypsyysarviointi.
- Ulkoinen arviointi – määrävälein tehtävä ulkoinen arviointi antaa puolueettoman kuvan organisaation kyberturvallisuuden tasosta ja tuottaa sille parannusesityksiä.

- Benchmarking eli ulkoisten edelläkävijä organisaatioiden löytäminen ja oman toiminnan vertaaminen heihin mahdollistaa parhaiden käytäntöjä omaksumisen toiminnan laadun kehittämisessä.

Laadullinen mittaaminen soveltuu hyvin toiminnan tilan ja siinä tapahtuvan muutoksen arviointiin. Siinä seurataan tyypillisesti toiminnan onnistumista. Määrällisessä mittaamisessa taas seurata tuotosten toteutumiseen käytettyä aikaa, kustannuksia, työajan menetyksiä sekä tietoturvapoikkeamien että kyberturvakoulutuksen määrää. Se soveltuu hyvin operatiivisen toiminnan mittaamiseen. (Valtiovarainministeriö 2006, 32)

Alla on esimerkkejä selkeistä operatiivisista kyberturvallisuuden tunnusluvuista, joita voit seurata ja helposti esitellä yrityksesi sidosryhmille. (SecurityScorecard 2019, Artikkeli)

- Valmiustaso: Kuinka monta verkossa olevaa laitetta on täysin kunnossa ja ajan tasalla?
- Tuntemattomat laitteet sisäverkossa: Kuinka monta tuntematonta laitetta on organisaation verkossa?
- Tunkeutumisyritykset: Kuinka monta kertaa organisaation verkkoon on yritetty tunkeutua?
- Keskimääräinen havaitsemisaika: Kuinka kauan kestää, että organisaatio saa tiedon mahdollisesta turvallisuushäiriöstä.
- Keskimääräinen ratkaisuaika: Kuinka kauan kestää, että organisaatio reagoi uhkaa, kun se saa siitä tiedon?
- Keskimääräinen palautusaika: Kuinka kauan organisaatiolta kestää toipua järjestelmän viasta?
- Päivityspäivät: Kuinka kauan organisaatiolta kestää suojauskorjausten käyttöönottoon?
- Kyberturvallisuustietoisuuskoulutuksen tulokset: Kuinka moni on osallistunut koulutukseen ja ymmärsivätkö he koulutuksen sisällön?
- Ilmoitettujen kyberturvallisuushäiriöiden määrä: Ilmoittavatko käyttäjät tiimillesi kyberturvallisuusongelmista?
- Käyttöoikeuksien hallinta: Kuinka monella käyttäjällä on järjestelmänvalvojan käyttöoikeudet?
- Suojauskäytäntöjen noudattaminen: Kuinka hyvin seurataan ja dokumentoidaan poikkeuksia, konfiguraatioita ja ohjeiden noudattamista?
- Kyberturvallisuustietoisuuskoulutus: Kuinka hyvin kyberturvallisuuskoulutusta koskevia asiakirjoja ylläpidetään? Onko koulutuksissa mukana kaikki organisaation jäsenet, myös ylin johto?
- Tapahtuman hinta: Kuinka paljon hyökkäykseen reagoiminen ja sen ratkaiseminen maksaa?

Tietoturvallisuuden mittaus on osa turvallisuuden hallintaprosessia ja luonteeltaan hyvin prosessimuotoista. Toistuvalla tietoturvallisuuden mittaamisella voidaan saada merkittävää hyötyä toiminnan turvallisuuden parantamisessa. (Valtiovarainministeriö 2006, 32)

Kyberturvallisuustyön johtamista ja siinä onnistumista voidaan arvioida usealla tasolla. Ylemmällä tasolla mittareita on vähemmän ja ne ovat strategiaa tukevia ja operatiivisella tasolla mittareita voi

olla enemmän ja ne ovat tarkempia. Operatiivisen tason mittareiden tulee auttaa strategisten tavoitteiden toteutumisen seurantaa. (Valtiovarainministeriö 2006, 32)

Jotta mittaamisesta tulisi toimiva käytäntö on käytettävän mittariston oltava yksinkertainen ja selkeä. Mittareita tulee olla mieluiten vähän mutta niiden tulisi olla kuvaavia sekä ohjaavia, kuin määrältään paljon ja kaikkea mahdollista mittaavia. (Valtiovarainministeriö 2006, 32)

5.3 Kyberturvallisuuden mittaristo ja sen kehittäminen

Kyberturvallisuuden mittariston tärkein tehtävä on raportoida käyttäjälle, miten kyberturvallisuuden kehittämisohjelman edellyttämät toimenpiteet ovat edenneet ja miten jatkossa eri kehitystoimenpiteitä tulisi edistää. (Lehto, Limnell jne, 66)

Kyberturvallisuuskyvykkyyden seurantaa ei ole olemassa vakioitua mittaustapaa. Mittareiden valinnalle onkin aluksi syytä asettaa tiettyjä perusvaatimuksia. Nämä mittaristolle kohdistuvia vaatimukset voidaan johtaa tarkasteltavan mittauskohteen osalta yleisistä mittaamisen näkökulmista. (Lehto, Limnell jne, 67)

Kyberturvallisuuden strategisen johtamisen raportissa listataan seuraavat perusvaatimukset kehitettävälle kyberturvallisuusmittaristolle:

1. Mittariston tulee auttaa organisaatiota päätöksenteossa.
2. Mittariston tulisi olla ymmärrettävä ja esitettävissä numeroin.
3. Mittariston tulisi vastata tavoiteltavia strategisia turvallisuustekijöitä.
4. Mittariston tulee pohjautua luotettavaan dataan.
5. Mittaristolla pitäisi olla yksinkertaista kerätä tarvittavia tietoja.
6. Mittaristoa tulisi pystyä ylläpitämään oman organisaation voimin.
7. Mittariston tulee olla diskreetti, jotta se tukee sen läpinäkyvyyttä ja sen kautta saatavien tietojen käytettävyyttä.
8. Mittariston tule mitata sellaisia asioita, joita halutaan seurata eikä ohjautua helposti saatavien tietojen mittaamiseen.
9. Mittariston laajuutta tulee pohtia tarkoin. Liian laaja mittaristo saattaa johtaa tarpeettoman mittaamiseen ja vääristää asioita tavoitetilan kannalta. (Lehto, Limnell jne, 67)

Tyypillisiä mittaristolla seurattavia asioita ovat esimerkiksi tietoturvapoikkeamat ja -toiminta ja niihin kohdistuvat muutokset. Näiden osalta voidaan mitata absoluuttisia arvoja ja näin seurata tietoturvatason kehittymistä.

Tietoturvatoiminnan mittarit

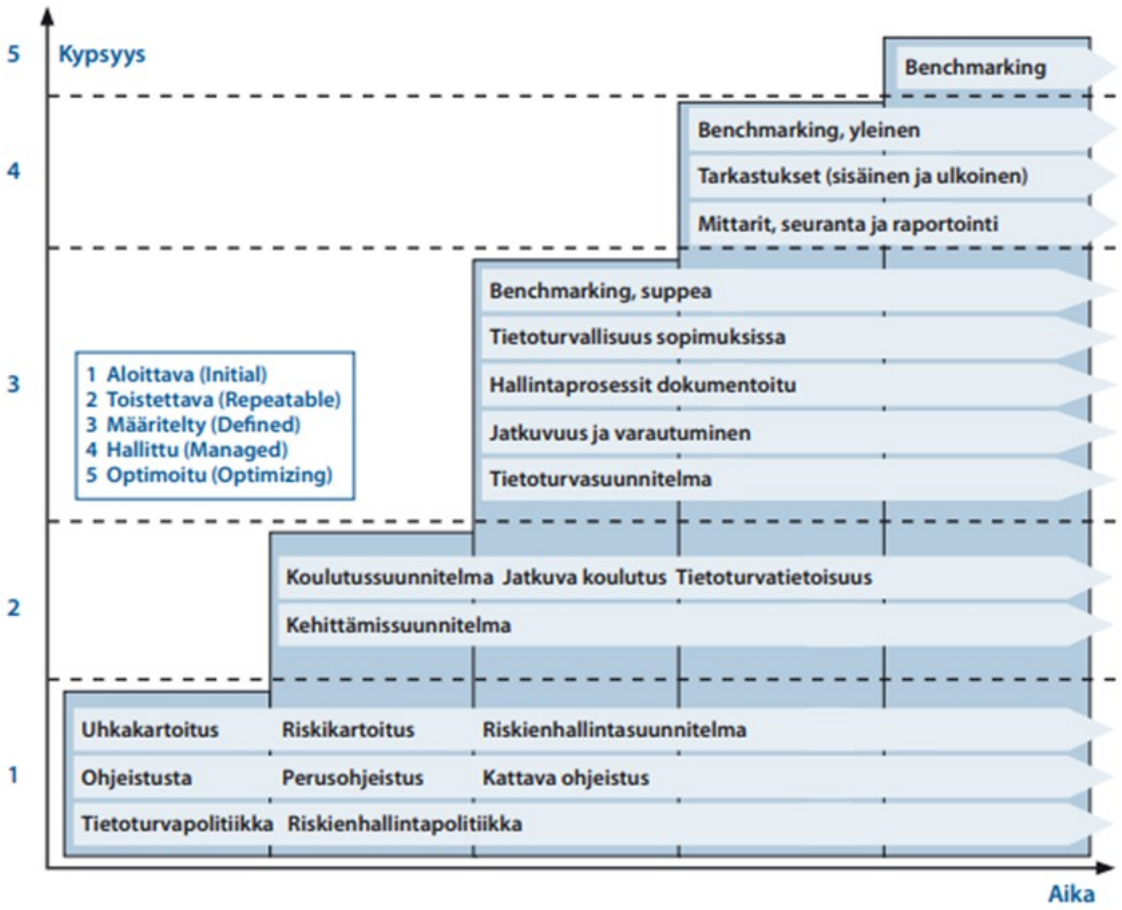
- Realisoituneet tietoturvapoikkeamat. Tavoitteena on mitata operatiiviselle toiminnalle aiheutuvaa haittaa ja saada tietoa tulevien tietoturvatoimenpiteiden suunnittelun avuksi.
- Tietoturvapoikkeamien hallinta. Tavoitteena on seurata toteutettujen tietoturvatoimenpiteiden tehokkuutta.

- Tietoturvatoimintaa raportoivia mittareita. Tavoitteena on mitata toiminnan tehokkuutta vertaamalla tehtyjä suoritteita ja käytettyihin panoksiin. (Valtiovarainministeriö 2006, 35)

Kyberturvallisuuden mittaamista voidaan arvioida myös organisaation tulostavoitteita vasten. Tällöin mitataan erikseen asetettujen tavoitteiden toteutumista, tietoturvapoikkeamia ja toimenpiteiden tehokkuutta. Lisäksi organisaation tulee säännöllisesti arvioida kyberturvallisuuden kypsyystasoa ja laatia sen perusteella uusi kehittämissuunnitelma, kunnes tavoiteltava taso on saavutettu.

Kokemus on osoittanut, että kyberturvallisuusmittareiden määrä yleensä vähenee niissä organisaatioissa, joissa kyberturvallisuuden kypsyystaso on jo korkeampi ja hallintamalli on jo pidemmälle kehittynyt. (Valtiovarainministeriö 2007, 42)

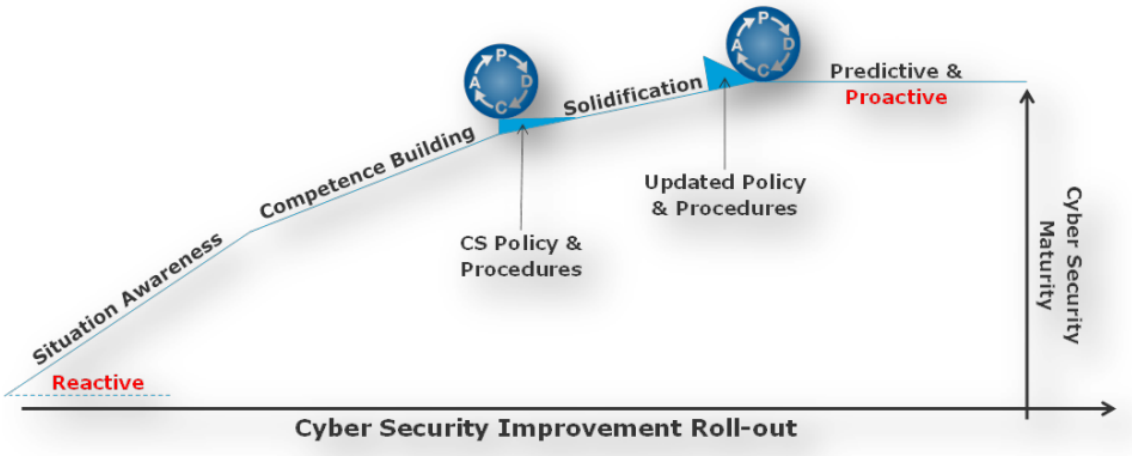
Mittaristo vaatii myös jatkuvaa päivittämistä, jotta sen antama tieto on todenmukaista ja toimintaa tukevaa. Kuvassa 25 on esimerkinomaisesti kuvattu kokemusperäisen kypsyysmallin soveltamisesta käytännössä.



Kuva 25. Esimerkki kypsyysmallin soveltamisesta käytännössä (Valtiovarainministeriö 2007, 42)

Organisaation kyberturvallisuuskypsyyden kehittymistä voidaan kuvata myös kuvan 26 mukaisesti. Kun kyberturvallisuutta kehittäviä toimenpiteitä suoritetaan jatkuvan parantamisen keinoin, kasvaa organisaation osaaminen ja toiminta muuttuu ajan myötä reaktiivisesta proaktiiviseksi toiminnaksi

kyberuhkia vastaan. Onnistuneen PDCA-muutoksen jälkeen saavutetaan korkeamman kypsyystaso ja siitä tulee lähtökohta seuraavien muutosehdotusten arvioinnissa.



Kuva 26. Organisaation kyberturvallisuuskypsyysaste kasvaa (DNV 2016, 29)

5.4 Traficomin Kybermittari

Suomessa organisaation kyberturvallisuuskypsyyden arviointiin on olemassa kansallinen Kyberturvallisuuskeskuksen kehittämä Kybermittari. ”Se näyttää, millä tasolla kyberriskien tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen ovat organisaatiossa. Kybermittari on räätälöity suomalaisten organisaatioiden tarpeisiin ja se pohjautuu kansainvälisiin kyberkyvykkyyksien mittausmalleihin (NIST Cybersecurity Framework sekä Cybersecurity Capability Maturity Model - C2M2). Kansallinen lähestymistapa mahdollistaa yritysten ja toimialojen yhtämittaisen vertailun ja tuo yhteisen kielen kyberturvallisuuden mittaamiseen ja kehittämiseen.” (Traficom 2020 5, 15)

Kybermittarin kautta organisaation johto saa nähtäväkseen ajantasaisen tilanteen oman vastuualueensa kyberriskien tunnistamiseen, havainnointiin, suojautumiseen ja turvallisuuspoikkeamatilanteesta palautumiseen. Kybermittarin arvioinnin perusteella voidaan tunnistaa ne kehitystoimenpiteet, joita organisaation tulee toteuttaa toimintansa kehittämiseksi ja suunnitellun tavoitetilan saavuttamiseksi. Kybermittarin käyttäminen on prosessi, jossa organisaation kyberturvallisuuden tasoa nostetaan, kunnes se vastaa haluttua kypsyystasoa. Kybermittarin arviointi vastaa aina vähintäänkin kahteen tärkeään kysymykseen: ”Mitä osa-alueita kyberturvallisuus nykyaikana sisältää?” ja ”Tiedämmekö mihin asioihin meidän tulisi seuraavaksi kiinnittää huomiota tai kohdentaa resursseja?” Kybermittarin avulla on mahdollista havaita myös aidosti liiketoimintaa uhkaavia kriittisiä puutteita, ilman laajempaa tai syvällisempää ymmärrystä kyber- tai tietoturvallisuudesta. (Traficom 2020 5, 15)

Kybermittari koostuu kuvan 27 mukaisesti kymmenestä osa-alueesta, joille jokaiselle on asetettu tavoitteita, joita pyritään täyttämään hyväksi havaituilla kyberturvallisuuden menettelytavoilla.

Kuva 27. Kybermittarin rakenne (Traficom 2020 5, 15)

Kybermittarin tulokset eli kypsyystasot esitetään viiden NIST Cybersecurity -viitekehyksen mukaisen kyvykkyyden mukaisesti: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen. (Traficom 2020 5, 15)

Kybermittarin kypsyystasot

- ”Taso 0 – Organisaatio toimii reaktiivisesti ja ei toteuta kyberturvallisuuden hallintaan liittyviä käytäntöjä.
- Taso 1 – Organisaatio toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä.
- Taso 2 – Organisaatiolla dokumentoidut säännöllisesti toistettavat ja ylläpidettävät kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet kyberturvallisuuden toteuttamiseksi on määritetty.
- Taso 3 – Organisaatio toimii ennakoivasti ja toteuttaa kyberturvallisuutta riskilähtöisesti, koko organisaation kattavia toimintamalleja ylläpidetään jatkuvasti ja kyberturvallisuudelle on määritetty tavoitteet, joita mitataan säännöllisesti.” (Traficom 2020 5, s. 15)

5.5 Kyberturvallisuuskyvykkyyden perustason vaatimukset

Organisaation kyberturvallisuuskyvykkyyden kehittäminen kannattaa aloittaa perustasosta. Hyökkääjät käyttävät usein tavallisia julkisesti saatavilla olevia sovelluksia ja menetelmiä, joista monet ovat torjuttavissa varmistamalla organisaation kyberturvallisuuden perustaso.

Kybermittari (Traficom 2020 4, itsearviointilomake) määrittelee kyberturvallisuuden perustasolle 1 seuraavia hallintatoimenpiteitä:

KYBERMITTARI

Kyberturvallisuuden kehitysalueet

Kyberturvallisuuden osioiden mukaisesti

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kypsyystasolle 1 vaadittavia toimenpiteitä

(ACCESS-1a) Työntekijöille ja muille entiteeteille (kuten prosesseille tai laitteille, jotka tarvitsevat pääsyn toimintoon kuuluviin laitteisiin, ohjelmistoihin tai tietovarantoihin) osoitetaan erilliset identiteetit. (Huom. tällä vaatimuksella ei kuitenkaan rajoiteta jaettujen identiteettien käyttöä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-1b) Työntekijöille ja muille entiteeteille jaetaan pääsyvaltuustiedot (kuten salasanat, älykortit tai avaimet). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-1c) Identiteetit poistetaan käytöstä, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-2a) Loogisten käyttöoikeuksien hallinnan valvontakeinoja on käytössä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-2b) Käyttöoikeudet poistetaan, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-3a) Fyysisen pääsynhallinnan valvontakeinoja on käytössä (kuten aitoja, lukkoja tai kyltejä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-3b) Pääsyoikeudet poistetaan, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ACCESS-3c) Pääsyoikeuksien käytöstä pidetään lokia. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ARCHITECTURE-1a) Organisaatiolla on suunnitelma tai strategia kyberarkkitehtuurin kehittämiselle (joka sisältää esimerkiksi kyberarkkitehtuurin tavoitteet, prioriteetit, vastuut ja seurannan). Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

(ARCHITECTURE-2a) Organisaation IT-järjestelmät on eriytetty mahdollisista OT-järjestelmistä segmentoimalla ne joko fyysisesti tai loogisesti. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä. [Tulkintaohje: mikäli OT-järjestelmä tai vastaavia ei ole, aseteta käytäntö "täysin toteutetuksi"]

(ARCHITECTURE-3a) Kyberturvallisuuden suojausmekanismeja on käytössä toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ARCHITECTURE-5a) Tallennettua arkaluontoista tietoa ("data at rest") suojataan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ASSET-1a) Toiminnon kannalta tärkeistä laitteista ja ohjelmistoista on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen laitteet ja ohjelmistot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

(ASSET-2a) Toiminnon kannalta tärkeistä tietovarannoista (kuten asiakastiedosta tai laitteiden ja ohjelmistojen perusasetuksista) on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen tietovarannot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

(ASSET-3a) Laitteiden, ohjelmistojen ja tietovarantojen konfiguraatioista on luotu vakioidut perusasetukset. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ASSET-4a) Rekistereihin kirjattuihin laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävät muutokset arvioidaan ja hyväksytetään ennen niiden toteuttamista. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(ASSET-4b) Rekistereihin kirjattuihin laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävistä muutoksista pidetään lokia. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(CRITICAL-1a) Organisaation tuottamat yhteiskunnalle kriittiset palvelut on tunnistettu ja dokumentoitu.

(CRITICAL-1b) (Yhteiskunnalle kriittisten) palveluiden tuottamiseen tarvittava data on tunnistettu ja dokumentoitu.

(CRITICAL-1c) Palveluiden tuottamiseen tarvittavat prosessit on tunnistettu ja dokumentoitu.

(CRITICAL-1d) Palveluiden tuottamiseen tarvittavat järjestelmät (IT- ja OT-omaisuus) on tunnistettu ja dokumentoitu.

(CRITICAL-2a) Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan (yhteiskunnalle kriittisten) palveluiden tuottamiseen, ovat organisaation turvallisuuden hallinnan politiikkojen ja prosessien piirissä.

(CRITICAL-2b) Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan yhteiskunnallisesti kriittisten palvelujen tuottamiseen, ovat organisaation riskienhallinnan politiikkojen ja prosessien piirissä.

(CRITICAL-3a) Organisaatiolla on kybertapahtumien ja -häiriöiden hallintasuunnitelma, joka kattaa kaikki (organisaation tuottamat yhteiskunnalle kriittiset) palvelut.

(CRITICAL-3b) Hallintasuunnitelma rajoittuu tunnettuihin hyökkäyksiin, mutta kattaa perusteellisesti näiden hyökkäysten todennäköiset vaikutukset.

(CRITICAL-3c) Kybertapahtumien ja -häiriöiden hallintaan osallistuva henkilöstö on sisäistänyt ja ymmärtää hallintasuunnitelman hyvin.

(CRITICAL-3d) Hallintasuunnitelma on dokumentoitu ja se jaetaan kaikille relevanteille sidosryhmille.

(PROGRAM-1a) Organisaatiolla on kyberturvallisuusstrategia. Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

(PROGRAM-2a) Resurssit (henkilöt, rahoitus ja työkalut) on osoitettu kyberturvallisuuden hallinnan perustamiseen. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(PROGRAM-2b) Organisaation ylin johto tukee kyberturvallisuuden hallintaa. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-1a) Havaitut kybertapahtumat raportoidaan ennalta määritellyille henkilöille tai roolien haltijoille ja niistä pidetään lokia. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-2a) Kyberhäiriöiden määrittämisestä on laadittu kriteeristö. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-2b) Kybertapahtumat analysoidaan siten, että se tukee mahdollisten kyberhäiriöiden määrittämistä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-3a) Kybertapahtumiin ja -häiriöihin reagoimista varten on tunnistettu soveltuvat työntekijät ja osoitettu heille heidän roolinsa. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-3b) Kybertapahtumiin- ja häiriöihin reagoidaan siten, että rajoitetaan toimintoon kohdistuvaa vaikutusta ja palautetaan toiminta normaaliksi. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-3c) Kyberhäiriöistä tuotetaan raportointia (esimerkiksi sisäisesti, CERT-FI tai soveltuville ISAC-ryhmille). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-4a) Organisaatio on kehittänyt toiminnan jatkuvuutta koskevat suunnitelmat, joiden avulla toiminnon toiminta voidaan säilyttää ja palauttaa, mikäli toimintaan kohdistuu kybertapahtuma tai -häiriö. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-4b) Tiedoista on saatavilla varmuuskopiot, joita testaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RESPONSE-4c) Varaosia tarvitsevat IT-laitteet (ja mahdolliset OT-laitteet) on tunnistettu. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RISK-1a) Organisaation kyberriskienhallintaa ohjaa suunnitelma (esimerkiksi strategia tai vastaava johtotason politiikka). Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

(RISK-2a) Kyberriskejä tunnistetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RISK-3a) Kyberriskit priorisoidaan niiden arvioidun vaikutuksen perusteella. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(RISK-4a) Riskeihin reagointikeinot (kuten riskin pienentäminen, hyväksyminen, välttäminen tai siirtäminen) ovat käytössä kyberriskeille ja kyberriskikategorioille. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(SITUATION-1a) Lokitietoa kerätään toiminnon kannalta tärkeistä laitteista, ohjelmistoista ja tietovarannoista [kts. ASSET-1a, ASSET-2a]. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(SITUATION-2a) Lokitietojen tarkastelua ja muuta kyberturvallisuusvalvontaa tehdään. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(SITUATION-2b) IT-ympäristöjä (ja mahdollisia OT-ympäristöjä) valvotaan poikkeavan toiminnan ja mahdollisten kybertapahtumien varalta. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THIRDPARTY-1a) Merkittävät kumppaniverkoston IT-riippuvuudet (ja mahdolliset OT-riippuvuudet) on tunnistettu (tällä tarkoitetaan sellaisia sisäisiä tai ulkoisia toimijoita, joista toiminto on riippuvainen - mukaan lukien toimintojen operoinnista vastaavat kumppanit). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THIRDPARTY-1b) Kumppaniverkoston toimijat, jotka omistavat, hallinnoivat tai pääsevät muutoin käyttämään toiminnon kannalta tärkeitä laitteita, ohjelmistoja tai tietovarantoja, on tunnistettu. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THIRDPARTY-2a) Toimittajien ja muiden kumppaniverkoston toimijoiden valintaan vaikuttaa arvio niiden kyberturvallisuuskelpoisuuksista. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THIRDPARTY-2b) Tuotteiden ja palveluiden valintaan vaikuttaa arvio niiden kyberkyvykkyyksistä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-1a) Haavoittuvuuksien tunnistamisen tueksi on tunnistettu soveltuvia tietolähteitä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-1b) Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-1c) Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-1d) Toiminnon kannalta olennaisiin haavoittuvuuksiin puututaan (esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-2a) Uhkien tunnistamisen tueksi on tunnistettu soveltuvia tietolähteitä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-2b) Uhkatietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(THREAT-2c) Toiminnon kannalta olennaisiin uhkiin puututaan (esimerkiksi lisäämällä valvontaa tai seuraamalla uhkien kehitystä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-1a) Toiminnon kyberturvallisuuteen liittyvät vastuut on tunnistettu. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-1b) Kyberturvallisuuteen liittyvät vastuut on osoitettu nimetyille henkilöille. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-2a) Kyberturvallisuuskoulutusta on saatavana sellaisille työntekijöille, joille on osoitettu kyberturvallisuuteen liittyviä vastuita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-2b) Kyberturvallisuuteen liittyvien tietojen, taitojen ja kykyjen vaatimukset ja niissä mahdollisesti ilmenevät puutteet on tunnistettu sekä nykyiset että tulevat tarpeet huomioiden. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-3a) Erilaisia tarkastuksia (esimerkiksi taustojen tarkistuksia, huumetestejä) suoritetaan uusia työntekijöitä palkatessa. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-3b) Työsuhteen päättymiseen liittyvissä menettelyissä huomioidaan kyberturvallisuus. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

(WORKFORCE-4a) Henkilöstön kyberturvallisuustietoisuutta kohotetaan erilaisin toimin. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

Kuva 28. Kybermittarin kypsyystasolle 1 vaadittavat toimenpiteet (Traficom 2020 4, itsearviointilomake)

6 TYÖN TULOKSET JA JOHTOPÄÄTÖKSET

Valtaosalla organisaatioista on yhä edelleen reagoiva toimintatapa kyberturvallisuuteen liittyvissä häiriötilanteissa, eli häiriötilanteissa ollaan yleensä tapahtuneen tosiasian edessä ja toimintaa leimaa nopeat päätelmät ja kiireelliset toimenpiteet. Kyberturvallisuuskyvykkyyden kehittämisen tavoitteena on luoda organisaatiolle edellytykset proaktiiviseen toimintaan reagoivan toiminnan sijasta.

6.1 Tärkeimmät tulokset ja johtopäätökset

Tämän opinnäytetyön tärkein tuotos AddSecurelle oli yleisen kyberturvallisuustietoisuuden lisääntyminen ja ymmärrys, mitkä eri osatekijät vaikuttavat organisaation kyberturvallisuuskyvykkyyteen. Opinnäytetyön aiheen merkityksellisyys korostui keväällä 2022, kun Venäjä hyökkäsi Ukrainaan ja tiedotusvälineet uutisoivat laajasti erilaisista organisaatioihin kohdistuvista kyberuhista.

Opinnäytetyön tutkimuksellisessa osuudessa suoritettujen Kybermittarin ja Katakrin itsearviointien perusteella saatiin hyvä tilannekuva organisaation nykyisestä kyberturvallisuuskypsyydestä. Arvioinnit helpottavat myös organisaation kyberturvallisuuskyvykkyyden jatkokehittämistä, koska jatkotoimenpiteet voidaan arviointien perusteella kohdistaa tehokkaammin oikeisiin asioihin.

Johtopäätöksenä opinnäytetyön teoriaosuudesta voidaan kyberturvallisuuden kehittämiseen keskeisimmin vaikuttaviksi hallintakeinoiksi listata seuraavat asiat:

- Johdon tuki - Ylimmän johdon tuki on ratkaisevan tärkeää organisaation kyberturvallisuuden kehittämisen kannalta.
- Kyberturvallisuuskoulutus - Kyberturvallisuuskoulutus ja tietoisuus ovat tärkeitä koko organisaatiolle ylimmästä johdosta työntekijöihin.
- Kyberturvallisuusmenettelyt ja ohjeet - Organisaation työntekijöillä on oltava selkeät menettelytavat, jotka määrittelevät miten kyberturvallisuutta hallitaan organisaatiossa.
- Organisaation kriittiset palvelut ja toiminnot - Organisaation on tunnistettava kaikki kriittiset palvelut ja toiminnot sekä niihin liittyvät järjestelmät, jotta voidaan tunnistaa riskit ja mahdolliset vaikutukset palvelujen toimintaan kyberturvallisuushäiriön sattuessa.
- Riskien arviointi - Kun organisaation kriittiset palvelut ja niihin liittyvät järjestelmät on tunnistettu ja dokumentoitu, on tehtävä riskinarviointi mahdollisten uhkien, riskien ja haavoittuvuuksien tunnistamiseksi.
- Riskien hallintasuunnitelma - Kun kriittiset palvelut, toiminnot ja niihin liittyvät järjestelmät sekä niihin liittyvät riskit on tunnistettu, seuraava vaihe on toteuttaa riskienhallintasuunnitelma, joka sisältää toimenpiteitä ja korjauksia tunnistettujen riskien hallitsemiseksi. Tämä vaihe perustuu riskinarviointiin, ja siinä hahmotellaan sekä menettelyt että tekniset toimenpiteet, jotka on toteutettava riskien minimoimiseksi ja korjaamiseksi.
- Kyberturvallisuusarkkitehtuuri - Organisaation dokumentoitu kyberturvallisuusarkkitehtuuri määrittelee, kuinka kyberturvallisuus toteutetaan organisaatiossa. Sen avulla kuvataan organisaation turvallisuusprosessien, kyberturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin.

- Toimitusketjun kyberturvallisuus – Kyberturvallisuus tulee huomioida toimitusketjun kaikilla tasoilla esimerkiksi organisaatioiden välisissä yhteistyösopimuksissa.
- Kyberturvallisuustapahtumien hallinta, reagointi ja toipuminen - Tehokkaan kyberturvallisuustapahtumien hallinnan avulla organisaatiot voivat tunnistaa kyberturvallisuuspoikkeamat ja reagoida nopeasti tapahtumaan ja toipua siitä, jotta se ei vaikuta palvelun turvallisuuteen.
- Kyberturvallisuusstandardit ja kehykset - Kyberturvallisuustyö tarvitsee tuekseen hyväksi koettuja hallintamalleja, joita ovat esimerkiksi NIST-kyberturvallisuuden viitekehys (NIST CSF) ja ISO 27001-standardi. Myös kansallinen Katakri 2020-ohjeistus tukee hyvin kyberturvallisuustyötä.
- Yhteistyö ulkoisten asiantuntijan kanssa - Yhteistyö kokeneen kyberturvallisuuskumppanin kanssa auttaa organisaatiota kehittämään nopeammin omaa kyberturvallisuuskyvykkyyttään.

Nämä edellä kuvatut kyberturvallisuuden hallintatoimenpiteet painottuvat organisaation toimintatapoihin, prosesseihin ja käytäntöihin sekä tietojärjestelmien hallintaprosesseihin. Näitä parantamistoimenpiteitä ei kannata tehdä yksittäin vaan niiden toteuttamisessa kannattaa hyödyntää kokonaisvaltaista lähestymistapaa. Käytännössä on havaittu, että paras tapa on luoda organisaatiolle kyberturvallisuuden hallintamalli, jossa kyberturvallisuus saadaan yhdistettyä työntekijöiden päivittäisiin tekemisiin, eivätkä toimenpiteet ole irrallisia toimenpiteitä.

Kyberturvallisuuden hallintamallin luominen kannattaa aloittaa pienin askelin, tavoitellen ensin perusasioiden kuntoon saamista. Hallintamallin luominen noudattaa tyypillisesti seuraavaa kehityspolkua.

1. Varmistetaan, että organisaation johto näkee kyberturvallisuustoimenpiteet strategisena tavoitteena ja valittujen toimenpiteiden toteutukseen saadaan riittävät resurssit.
2. Päivitetään organisaation toimintapolitiikka valitun kyberturvallisuusstrategian edellyttämällä tavalla.
3. Kasvatetaan henkilöstön kybertietoisuutta, koska suurin osa organisaatioiden kyberturvallisuusloukkauksista johtuu inhimillisestä erehdyksestä.
4. Valitaan kyberturvallisuustyön hallintamalliksi ja toimenpiteiden tueksi sopiva kyberturvallisuutta tukeva viitekehys esimerkiksi NIST CSF-kyberturvallisuuden viitekehys tai ISO 27001-standardi.
5. Suoritetaan organisaatiolle Kyberturvallisuuskypsyyden lähtötason arviointi ja suoritetaan arvioinnin osoittamat puutteet. Esimerkiksi Kyberturvallisuuskeskuksen Kybermittarin kypsyysarvio osoittaa selkeästi ne toimenpiteet, joihin organisaation tulee panostaa tavoitellessaan parempaa kyberturvallisuuskyvykkyyttä.
6. Luodaan kyberturvallisuuden kehitystoimenpiteistä jatkuva prosessi valitsemalla seuraavan kehityskierroksen kohteet ja -toimenpiteet aina uuden Kybermittarin kypsyysarvioinnin tuloksista ja suoritetaan ne.

7. Seurataan kyberturvallisuustoimenpiteiden vaikuttavuutta osana organisaation johtamista. Tämä voi tapahtua esimerkiksi Kybermittarin osoittamalla tavalla. Tämän lisäksi voidaan valita muutama erillinen KPI-mittari, jotka seuraavat esimerkiksi organisaation tietoturvapoikkeamia, tietoturvatoimintaa sekä niissä tapahtuneita muutoksia.

Tämän opinnäytetyön teoriaosuuteen koottua tietoa on hyödynnetty varsinaisten AddSecurelle ehdotettujen kehitystoimenpiteiden määrittämisessä. Organisaation kyberturvallisuuskyvykkyyden nykytila-arvio ja siitä johdetut tuotokset eli ehdotukset kehittämistoimenpiteiksi on kuvattu tarkemmin tämän opinnäytetyön liitteissä 1–3 ja ne on jätetty työn luottamuksellisuuden vuoksi pois julkaistavasta versiosta. Liitteet on luovutettu ainoastaan opinnäytetyön toimeksiantajalle.

6.2 Onnistumiset ja haasteet

Opinnäytetyö täytti sille asetetut tavoitteet. AddSecuren kyberturvallisuus osaaminen kasvoi ja löysimme konkreettiset kehityskohteet kyberturvallisuuskyvykkyyden kehittämiseksi.

Myös ensikokemukset Kybermittarista olivat hyvin positiiviset. Kybermittarin hyödyntämistä esimerkiksi kerran vuodessa tapahtuvaksi organisaation kyberturvallisuuskyvykkyyden itsearvioinniksi tullaan ehdottamaan organisaation johtoryhmälle. Kybermittarista saadaan paras hyöty esille, kun se otetaan osaksi toiminnan jatkuvaa kehittämistä. Suositeltavaa on myös, että arviointi sulautetaan osaksi organisaation kokonaisvaltaista riskienhallintaa ja arvioinnin perusteella tehtävä kyberturvallisuuden kehittämistehtävät osaksi organisaation muuta kehittämistoimintaa.

Kyberturvallisuustyön alkuvaiheessa haasteena on usein myös resurssointi. Kannattaakin miettiä heti alussa turvautumista organisaation ulkopuolisiin konsultteihin jo pelkästään sen takia, että oma henkilöstö sitoutuu lähes kokonaisuudessa päivittäiseen operatiiviseen toimintaan. Organisaation ulkopuolisen resurssin käyttö on kannatettavaa myös kyberturvallisuuteen liittyvän tietotaidon hankinnan näkökulmasta katsottuna.

6.3 Jatkokehitystarpeet

Tämän opinnäytetyön tavoitteena oli selvittää millaisia toimenpiteitä tiedon suojaaminen edellyttää, jotta organisaation kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvata niin normaali kuin myös poikkeusolosuhteissa. Organisaation kyberturvallisuuden kehitystyö jatkuu nyt opinnäytetyön jälkeen pienempinä sisäisinä kehitysprojekteina normaalin päivätyön puitteissa. Ensimmäisenä tavoitteena on hyödyntää itsearviointien tuloksia ja korjata havaittuja puutteita organisaation kyberturvallisuustoiminnassa.

Kehitystoimenpiteiden hallintaa helpottaa, jos ne määritellään pieniksi kehitysprojekteiksi, jolloin niihin tarvittavat henkilöt, rahat ja aikataulut kohtaavat paremmin ja kehitystyöllä on selkeä alku ja loppu. Jokaiselle yksittäisille kehitystoimenpiteille kannattaa laatia suppea projektisuunnitelma, joka

voi olla esimerkiksi kuvan 29 kaltainen yhden sivun projektikooste. Se kokoaa yhteen projektin keskeisimmät asiat ja auttaa myös kehitystoimenpiteiden seurannassa, koska samanaikaisesti voi olla käynnissä useampia kehitystoimenpiteitä ja ne saattavat kilpailla samoista projektiresursseja. Jos näitä kehitettäviä asioita on useita, niin kokonaisuuden hallinnan kannalta voi olla järkevää luoda yksi projektit yhteen kokoava pääprojekti, jonka alle kaikki pienemmät projektit sitten sijoittuvat.

Kuva 29. Esimerkki pienestä projektikoosteesta

6.4 Jatkotutkimusaihe

Tämän opinnäytetyön jatkotutkimusaiheeksi voisi muodostua sopivan kyberturvallisuusmittariston kehittäminen ja käyttöönotto. Toimiva mittaristo auttaa niin johtoa kuin operatiivista henkilöstöä seuraamaan toteutettavia kyberturvallisuuden hallintatoimenpiteitä ja niiden tehokkuutta. Kehitystyö olisi hyvä jatko tämän opinnäytetyön tutkimukselliselle osuudelle, joka suoritettiin valtaosin ryhmätyönä. Tällaiset mittaristojen kehityshankkeet toteutetaan tyypillisesti myös ryhmätyönä. Yhteistyönä luotava mittaristo syventäisi myös henkilöstön kyberturvallisuusosaamista ja ymmärrystä siitä, mitkä tekijät vaikuttavat mittariston osoittamaan tietoon.

Lönnqvist jne. (Lönnqvist ym. 2006, 105) kuvaavat, että mittariston suunnittelun perustana tulee olla aina jokin tarve mittaamiseen. Jos organisaatiossa ei tunnista tätä syytä suorituskyvyn mittaamiseen, mittaristohanketta ei kannata käynnistää. Kun mittaristohanke nähdään hyödylliseksi, henkilöstö sitoutuu paremmin sen toteuttamiseen. Mittariston suunnittelu kannattaa tehdä ryhmätyönä. Hankkeen kannalta on keskeistä, että projektiin osallistuvat avainhenkilöt eri puolilta organisaatiota. Johdon on sitouduttava hankkeeseen ja henkilöstön mielipidettä ja asiantuntemusta tarvitaan.

7 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää, mistä osatekijöistä kyberturvallisuuden hallintamalli koostuu ja millainen sen tulee olla, jotta se täyttää viranomaisten perustason vaatimukset luottamuksellisen tiedon suojaamisen osalta.

Opinnäytetyön teoriaosuudessa tutustuttiin laajasti niin kotimaiseen kuin ulkomaiseen kyberturvallisuutta koskevaan tietoaineistoon. Näin korona-aikana tiedonsaantia helpotti suuresti se, että tuorein kyberturvallisuusaineisto löytyi parhaiten sähköisesti internetistä. Tämän aineiston pohjalta koottiin yhteen ne keskeiset kyberturvallisuuden hallintaan vaikuttavat tekijät, joita kehittämällä organisaatio voi vaikuttaa kyberturvallisuuskyvykkyyteensä.

Opinnäytetyössä teoriaosuudessa kartoitettiin myös NIST:n kyberturvallisuuden CSF-viitekehyksen pohjalta hyväksi havaittuja kyberturvallisuuden hallintakeinoja, joita toteuttamalla organisaatio pystyy kehittämään kyvykkyyttään kyberhäiriötilanteiden tunnistamisen, suojautumisen, havaitsemisen, reagoimisen sekä palautumisen osalta.

Jotta kyberturvallisuuskyvykkyyden kehittymistä voidaan seurata ja ohjata, tarvitaan tähän sopiva mittari. Opinnäytetyön tutkimuksellisessa osuudessa organisaatiolle tehtiin kyberturvallisuuskypsyyden nykytila-arvio Kyberturvallisuuskeskuksen kybermittarin avulla. Arvio tehtiin sisäisesti ja siihen osallistui useita organisaation työntekijöitä. Kybermittari osoittautui hyväksi työvälineeksi kyberturvallisuuskypsyyden arviointiin ja se huomioi kysymyksillään laajasti eri kyberturvallisuuteen vaikuttavat osa-alueet. Kybermittaria tullaan hyödyntämään jatkossa myös vuosittaisiin organisaation kyberturvallisuuskypsyyden arviointeihin, koska se osoittaa konkreettisesti ne kehityskohteet, joihin organisaation tulee seuraavaksi puuttua.

Lopputuloksena niin AddSecurelle kuin opinnäytetyön tekijälle syntyi hyvä käsitys kyberturvallisuuden hallintaan vaikuttavista tekijöistä ja selkeä näkemys niistä kehitystoimenpiteistä, jotka suorittamalla organisaatio saavuttaa tavoitellun kypsyystason kyberturvallisuuden kehittämisen portaikossa. Hyvä oppi oli myös ymmärtää, kuinka moni eri osa-alue vaikuttaa organisaation kyberturvallisuuskyvykkyyteen, kuin myös se, että kyberturvallisuuskyvykkyyden kehittäminen on jatkuva prosessi, joka ei koskaan tule täysin valmiiksi.

LÄHTEET

ADDSECURE 2021. Yrityksen internet-sivut. [Viitattu 2021-11-27]. Saatavissa: https://www.addsecure.fi/

BALBIX 2022. Artikkeli: Operationalize the NIST Cybersecurity Framework Without Pulling All Your Hair Out. [Viitattu 2022-01-07]. Saatavissa: https://www.balbix.com/blog/operationalize-nist-cybersecurity-framework/

CICHONSKI Paul, MILLAR Tom, GRANCE Tim, SCARFONE Karen (2012). Computer Securitys Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. NIST. [Viitattu 2021-11-27]. Saatavissa: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

CINIA 2022. Artikkeli: Kyberturvallisuus on ennakointia, havainnointia ja jatkuvuuden hallintaa. [Viitattu 2022-01-07]. Saatavissa: https://www.cinia.fi/blogi/kyberturvallisuus-ennakointia-havainnointia-ja-jatkuvuuden-hallintaa

CSOONLINE 2021. Artikkeli: Top cybersecurity statistics, trends, and facts. [Viitattu 2022-03-07]. https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

CYBERTALK 2021. Artikkeli: Alarming cyber security facts to know for 2021 and beyond. [Viitattu 2022-03-07]. https://www.cybertalk.org/2021/12/02/alarming-cyber-security-facts-to-know-for-2021-and-beyond/

CYBINSOLUTIONS 2022. Artikkeli: 15 Alarming Cyber Security Facts and Stats. [Viitattu 2022-03-07]. Saatavissa: https://www.cybintsolutions.com/cyber-security-facts-stats/

DIGI- JA VÄESTÖTIETOVIRASTO 2021. Digiturvallisuuden hallinta – tukimateriaali digiturvan kehittäjille. [Viitattu 2021-11-27]. Saatavissa: https://dvv.fi/documents/16079645/0/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf/f6243645-79e2-81f7-5c3d-ccf2e972b2ec/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf?t=1622534350192

DNV 2022. Maritime cyber security. [Viitattu 2022-01-07]. Saatavissa: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html

DNV 2016. Cyber security resilience management for ships and mobile offshore units in operation. [Viitattu 2022-01-23]. Saatavissa: https://brandcentral.dnvgl.com/download/DownloadGateway.dll?h=BE1B38BB718539CC0AB58A5FF2EA7A83DE6D49BC96B8DB13C4CAAFA95E9ACCDA9F12593F5BB9D3D16F4B2EB2FF9780D9

ENISA 2021. Enisa Threatlandscape 2021 April 2020 to mid-July 2021. [Viitattu 2022-01-07]. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

ETLA 2020. Artikkeli: Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? [Viitattu 2022-03-07]. https://www.etla.fi/julkaisut/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/

FINANCESONLINE 2021. Artikkeli: 119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis. [Viitattu 2022-03-07]. https://financesonline.com/cybersecurity-statistics/

FINNISH INFORMATION SECURITY CLUSTER 2022. Artikkeli: Muista jatkuvuus, muutoin se voi unohtaa sinut – kyberturvallisuus on keskeinen osa digitaalista liiketoimintaa. [Viitattu 2022-01-07]. Saatavissa: https://www.fisc.fi/muista-jatkuvuus-muutoin-se-voi-unohtaa-sinut-kyberturvallisuus-on-keskeinen-osa-digitaalista-liiketoimintaa/

HARRIS Shon, MAYMI Fernando 2016, CISSP Exam Guide Seventh Edition. New York: McGraw-Hill Education.

HUOLTOVARMUUSKESKUS 2021. Artikkeli: Toimialat kehittämään omaa kyberturvallisuuttaan. [Viitattu 2021-11-27]. Saatavissa: https://www.varmuudenvuoksi.fi/aihe/elintarvikehuolto/547/toimialat_kehittamaan_omaa_kyberturvallisuuttaan

HUOLTOVARMUUSORGANISAATION DIGIPOOLI 2020. Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot. [Viitattu 2021-11-27]. Saatavissa: https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

IBM 2020. Raportti: Cost of a Data Breach Report 2020. [Viitattu 2022-03-07]. https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

ICT INSTITUTE 2017. Information security and PDCA (Plan-Do-Check-Act). [Viitattu 2022-01-07]. Saatavissa: https://ictinstitute.nl/pdca-plan-do-check-act/

KESKUSKAUPPAKAMARI 2021. Tietoturvaopas yrityksille. [Viitattu 2021-11-27]. Saatavissa: https://www.doaudit.fi/tietoturvaopas/

LEHTO Martti, LIMNELL Jarno, KOKKOMÄKI Tuomas, PÖYHÖNEN Jouni, SALMINEN Mirva (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. [Viitattu 2021-11-27]. Saatavissa: https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf

LIMNELL Jarno, MAJEWSKI Klaus, SALMINEN Mirva (2014). Kyberturvallisuus. Jyväskylä: Docendo Oy ja kirjoittajat

LÖNNQVIST Antti, KUJANSIVU Paula, ANTIKAINEN Riikka (2006). Suorituskyvyn mittaaminen – Tunnusluvut asiantuntijaorganisaation johtamisvälineenä. 2. painos. Helsinki: Edita Publishing Oy

NIST 2018. Framework for Improving Critical Infrastructure Cybersecurity. [Viitattu 2021-11-27]. Saatavissa: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST 2018 1. Cybersecurity Framework v1.1 core [Viitattu 2022-01-07]. Saatavissa: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2F2018%2F04%2F17%2F2018-04-16_framework_v1.1_core1.xlsx&wdOrigin=BROWSELINK

OJATSALO Katri, MOILANEN Teemu, RITALAHTI Jarmo (2015). Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan (3.–4. painos). Helsinki: Sanoma Pro Oy.

OPSEC 2021. Kiristysohjelma lukitsee tietokoneen – älä koskaan maksa rikollisille. [Viitattu 2021-11-27]. Saatavissa: https://www.opsec.fi/fi/2018/06/20/kiristysohjelma-lukitsee-tietokoneen-ala-koskaan-maksa-rikollisille/

PURPLESEC 2021. Artikkeli: Cyber securitys trends in 2021. [Viitattu 2022-03-07]. Saatavissa: https://purplesec.us/cyber-security-trends-2021/

PWC 2022. Artikkeli: Olethan huomioinut kyberturvallisuuden sisäisessä valvonnassa? [Viitattu 2022-01-07]. Saatavissa: https://uutishuone.pwc.fi/olethan-huomioinut-kyberturvallisuuden-sisaisessa-valvonnassa

ROUSKU Kimmo (2014). Kyberturvaopas: Tietoturvaa kotona ja työpaikalla. Viro: Talentum Media Oy ja Kimmo Rousku

SECURITY AFFAIRS 2022. Artikkeli: NIST CyberSecurity Framework. [Viitattu 2022-01-07]. Saatavissa: https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html

SECURITYSCORECARD 2019. Top 20 Cybersecurity KPIs to Track in 2021. [Viitattu 2022-01-07]. Saatavissa: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track

SFS-EN ISO 27000:2020 Tietoturvallisuuden hallintajärjestelmät

SUOMIDIGI 2012. Teknisen ICT-ympäristön tietoturvataso-ohje. [Viitattu 2021-11-27]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_3_2012_pdf.pdf

SUOMIDIGI 2021. Vahti-ohjeet. [Viitattu 2021-11-27]. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

SUOMIDIGI 2014. Tietoturvallisuuden arviointiohje Vahti 2/2014. [Viitattu 2021-11-27]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2014_pdf_0.pdf

TEKNOLOGIATEOLLISUUS 2021. Tieto- ja kyberturvallisuus. [Viitattu 2021-11-27]. Saatavissa: https://teknologiateollisuus.fi/sites/default/files/inline-files/T-Tieto-ja-kyberturvallisuus.pdf

TRAFICOM 2019. Riskienhallinnan (hyvin) lyhyt oppimäärä [Viitattu 2022-01-07]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskienhallinnan-hyvin-lyhyt-oppimaara

TRAFICOM 2020 1. Katakri – tietoturvallisuuden auditointityökalu viranomaisille 2020. [Viitattu 2021-11-27]. Saatavissa: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

TRAFICOM 2020 2. Kybermittari Kansallinen kyberturvallisuuden arviointimalli. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

TRAFICOM 2020 3. Suositus kyberturvallisuuden edistämisestä raideliikenteessä. [Viitattu 2021-11-27]. Saatavissa: https://www.traficom.fi/sites/default/files/media/regulation/Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4.pdf

TRAFICOM 2020 4. Kybermittari kyberturvallisuuden arviointityökalu. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Arviointityokalu_V2_luonnos09.xlsx

TRAFICOM 2020 5: Kybermittari – esittely. [Viitattu 2022-01-07]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_v1.pdf

TRAFICOM 2021. Kybersää syyskuu 2021. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_syyskuu_2021_TLP_WHITE.pdf

TRAFICOM JULKAISUJA 2/2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

TRAFICOM JULKAISUJA 228/2020. Pienyrityksen kyberturvaopas. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

TRAFICOM 2022. Artikkeli: Tietojärjestelmille on asetettava tietojen suojaamisen mukaiset vaatimukset. [Viitattu 2022-01-07]. Saatavissa: https://www.traficom.fi/fi/ajankohtaista/blogit/tietojarjestelmille-asetettava-tietojen-suojaamisen-mukaiset-vaatimukset

TURVALLISUUSKOMITEA 2017. Kodin kyberopas -Ohjeita digitaaliseen arkeen. [Viitattu 2021-11-27]. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf

TURVALLISUUSKOMITEAN SIHTEERISTÖ 2013. Suomen kyberturvallisuusstrategia. [Viitattu 2021-11-27]. Saatavissa: https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30

TURVALLISUUSKOMITEA 2022. Artikkeli: Uhkat. [Viitattu 2022-01-07]. Saatavissa: https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/uhkat/

TURVALLISUUSKOMITEA 2022 1. Ennakointi ja varautuminen. [Viitattu 2022-01-15]. Saatavissa: https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ennakointi-ja-varautuminen/

YLE 2022. Artikkeli: Savonia-ammattikorkeakouluun tehty massiivinen tietoturvahyökkäys – kiristysohjelma lukinnut tietoja. [Viitattu 2022-03-07]. https://yle.fi/uutiset/3-12302764

VALTIOVARAINMINISTERIÖ 2005, Tietoturvapoikkeamatilanteiden hallinta. Helsinki 2005. [Viitattu 2022-01-07]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2005.pdf

VALTIOVARAINMINISTERIÖ 2006. Vahti 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen. [Viitattu 2022-01-07]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_6_2006.pdf

VALTIOVARAINMINISTERIÖ 2007, Vahti 3/2007 Tietoturvallisuudella tuloksia. [Viitattu 2022-01-07]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2007.pdf

VALTIOVARAINMINISTERIÖ 2016. Vahti 2/2016 Toiminnan jatkuvuuden hallinta. [Viitattu 2022-01-07]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf

VALTIOVARAINMINISTERIÖN JULKAISUJA 8/2017. Tietoturvapoikkeamatilanteiden hallinta. [Viitattu 2022-01-23]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf

VALTIOVARAINMINISTERIÖN JULKAISUJA 22/2017. Ohje riskienhallintaan 2017. [Viitattu 2021-11-27]. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf

VIESTINTÄVIRASTO 2014. Kohdistettujen haittaohjelmahyökkäysten uhka on otettava vakavasti. [Viitattu 2021-11-27]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

VERIZON 2021. Raportti: Breach Investigations Report (DBIR). [Viitattu 2022-03-07]. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

VTT 2009, PK-yrityksen riskienhallinta. [Viitattu 2021-11-27]. Saatavissa: http://virtual.vtt.fi/virtual/pkrh/startti-riskienhallintaan/mita-riskienhallinta-on/riskienhallintaprosessin-vaiheet.html

VÄESTOREKISTERIKESKUS 2019. Digiturvaopas - Judo-hanke sekä digitaalinen turvallisuus toiminnan mahdollistajana. [Viitattu 2021-11-27]. Saatavissa: https://dvv.fi/documents/2252790/13076333/Digiturvaopas_1206_2019.pdf/f8d7e2ab-7395-2e4a-88e9-291cea4d0b41/Digiturvaopas_1206_2019.pdf

LIITE 1 KYBERTURVALLISUUDEN NYKYTILA-ANALYYSI

Opinnäytetyön salainen osa.

LIITE 2 TULOSTEN ARVIOINTI

Opinnäytetyön salainen osa.

LIITE 3 KEHITYSEHDOTUKSET

Opinnäytetyön salainen osa.