DIGI- JA VÄESTÖTIETO-VIRASTO

Kuntien tietoturvavalvomoiden toimintamalli

Selvitys

20.10.2023

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

Kuntien tietoturvavalvomoiden toimintamalli

1 Tiivistelmä

Digi- ja väestötietovirasto toteutti vuonna 2023 selvityksen kuntien digitaalisten toimintaympäristöjen tietoturvavalvomo-toiminteesta sekä sen järjestämistavoista osana Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmaa 2020–2023 (Haukka). Selvityksessä kartoitettiin tietoturvavalvomoiden hyödyntämisen nykytilaa kunnissa sekä vaihtoehtoisia toimintamalleja tietoturvavalvomoiden järjestämiseen, hyödyntämiseen ja tietoturvatietojen tiedonvaihdon kehittämiseen kunnissa.

Tiedot kerättiin maaliskuussa-kesäkuussa 2023 toteutetuilla työpajoilla, turvalomakekyselyllä ja haastatteluilla. Työpajoihin, kyselyyn ja haastatteluihin osallistui 122 kuntaa sekä tietoturvavalvomopalveluiden tarjoajia.

Nykytilassa kuntien tietoturvavalvomoiden toteutuksissa on laajaa vaihtelua. Kaikilla kunnilla ei ole käytössään tietoturvavalvomoa. Osa tietoturvavalvomoista on kunnan itse tuottamia, kun taas osa on kuntien omistamanien inhouse-yhtiöiden tuottamia palveluita tai yksityisten palveluntarjoajien palveluita.

Selvityksessä havaitut olennaisimmat esteet tietoturvavalvomoiden laajamittaiselle hyödyntämiselle kunnissa olivat tietoturvabudjettien riittämättömyys sekä tietoturvan valvontaan liittyvän osaamisen puute. Lisäksi haasteita aiheuttaa hankintaosaamisen ja markkinatuntemuksen puute sekä puutteet tietoturvan perusasioissa.

Kunnat kaipaavat erityisesti informaatio-ohjausta ja suosituksia sekä rahoituksellista tukea tietoturvavalvomoiden hyödyntämiseksi. Kuntien tietohallinnoissa oli vahva ymmärrys tietoturvavalvomon tarpeellisuudesta ja hyödyistä, mutta hyötyjen kommunikointi ylimmälle johdolle ja päätöksentekijöille on paikoin ollut haastavaa. Viranomaisten laatimat ohjeistukset ja painokkaat suositukset koettiin yhtenä keskeisistä keinoista perustella tietoturvan valvonnan kehittämistä kunnissa.

Valtakunnallisen, keskitetyn tietoturvavalvomon perustamisen olennaisimmat haasteet liittyvät kuntien vaihtelevaan tietoturvan kypsyystasoon sekä vaihtelevaan tapaan järjestää tietohallinnon toiminnot, kuten palvelut, tietoliikenneinfrastruktuuri ja tietojärjestelmät.

Kuntien kannattaakin hyödyntää tietoturvan valvonnassa esimerkiksi olemassa olevia palveluntuotantoverkostojaan. Kaikkein pienimmillä kunnilla ei ole välttämättä mahdollisuutta perustaa tai ulkoistaa tietoturvavalvomoa itsenäisesti. Alueelliset toteutukset ja yhteishankinnat olisivat hyödyksi erityisesti siinä tapauksessa, jossa alueen kuntien palvelutuotannossa on muutenkin yhtäläisyyksiä.

Tiedonvaihdon keskeisiä tarpeita kuntaorganisaatiolle ovat tietoturvan valvontaan liittyvien ajantasaisten uhkatietojen vaihto sekä tietoturva- ja tietosuojapoikkeamiin liittyvä raportointi tarvittaville viranomaistahoille. Tiedonvaihdon tehokas järjestäminen vaatii kunnilta ja niiden palveluntuottajilta aktiivista osallistumista tiedonvaihtoverkostoihin ja -kanaviin.

2 Johdanto

2.1 Selvityksen taustat ja tavoitteet

Valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä. [1]

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020–2023 (Haukka) kuvataan periaatepäätöksen toteuttaminen. Haukka-hanke sisältää 19 tehtävää, joita toteutetaan yhteistyössä kuntien, Kuntaliiton ja valtion viranomaisten kanssa. Keskeisiä kehitettäviä palveluita ovat mm. julkisen hallinnon digitaalisen turvallisuuden riskien hallinta, tietoturvallisuuden arviointi ja tekninen valvonta sekä kunnille tarkoitetut yhteiset, digitaalista turvallisuutta edistävät palvelut. [2]

Digi- ja väestötietovirasto toteutti vuonna 2023 selvityksen kuntien digitaalisten toimintaympäristöjen tietoturvavalvomo-toiminteesta sekä sen järjestämistavoista osana Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka).

Selvityksessä kartoitettiin tietoturvavalvomoiden hyödyntämisen nykytilaa kunnissa sekä vaihtoehtoisia toimintamalleja tietoturvavalvomoiden järjestämiseen, hyödyntämiseen ja tietoturvatietojen tiedonvaihdon kehittämiseen kunnissa.

Tässä raportissa käydään läpi tietoturvavalvomotoiminnon olennaisimmat elementit, kuntien tietoturvavalvomotoimintojen nykytila, vaihtoehtoisia kuntien tietoturvavalvomotoiminnan järjestämistapoja, sekä esitetään laaja joukko erilaisia konkreettisia toimenpiteitä, joilla tietoturvan valvontaa voidaan kehittää kunnissa.

Selvitys tehtiin yhteistyössä muun muassa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen, tietoturvavalvomo- ja havainnointipalveluita tuottavien yritysten sekä kuntien kanssa.

2.2 Selvityksen toteutus

Selvitys toteutettiin keräämällä tietoa ja näkemyksiä liittyen kuntien tietoturvavalvomotoimintojen järjestämiseen sekä kehittämiseen kattavasti eri kanavia ja sidosryhmiä hyödyntäen. Selvityksen aikana toteutettuja erilaisia tiedonkeruutapoja olivat:

- Kansainvälinen katsaus, jossa tarkasteltiin valikoitujen valtioiden julkisen hallinnon tietoturvavalvomotoimintoja julkisista lähteistä saatavissa olevan tiedon perusteella,

[1] Julkisen hallinnon digitaalinen turvallisuus, Valtiovarainministeriön julkaisuja 2020:23
[2] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka), Valtiovarainministeriön julkaisuja 2020:33

- aikaisemmat aiheeseen liittyvät raportit ja selvitykset,
- yhteistyöpajat tietoturvapalveluita tarjoavien palveluntarjoajien sekä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen kanssa
- kuntien suorat haastattelut,
- kunnille toimitettu verkkolomakekysely sekä
- palveluntarjoajille toimitettu verkkolomakekysely.

Selvitykseen liittyvä tietojen kerääminen ajoittui pääasiallisesti ajalle tammikuu 2023 – kesäkuu 2023.

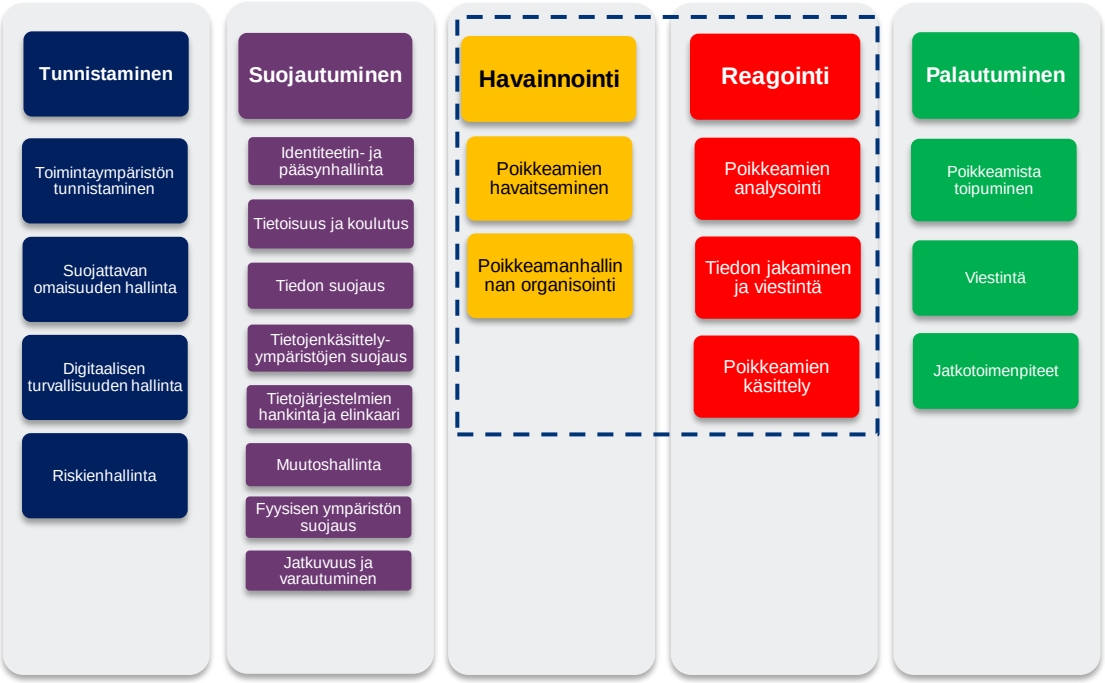
2.3 Tietoturvavalvomo osana digitaalisen turvallisuuden arkkitehtuuria

Digitaalisen turvallisuuden arkkitehtuuri, joka esitetään kuvassa 1, koostuu organisaation digitaalisen turvallisuuden rakennusosista kuten toimintatavoista ja teknisistä ratkaisuista sekä niiden suhteesta organisaation tavoitteisiin ja toimintaan. [3]

Havainnointi ja siihen liittyvät tekniset ja operatiiviset ratkaisut, kuten tietoturvavalvomo, muodostavat olennaisen osan digitaalisen turvallisuuden arkkitehtuuria, sillä sen avulla poikkeamat digitaalisen turvallisuuden perustasosta havaitaan mahdollisimman varhaisessa vaiheessa ja niihin voidaan reagoida valmiiksi määritellyn poikkeamanhallinnan prosessin mukaisesti.

Poikkeavien tapahtumien havaitseminen digitaalisissa toimintaympäristöissä vaatii usein etenkin päätelaitteiden, tietoverkkoinfrastruktuurin ja palveluiden tuottamaa tietoa ja sen analysointia. Valvonnan tuleekin kohdistua sekä organisaation itse ylläpitämiin, että ulkoistettuihin tai palveluina ostettuihin organisaation toiminnalle olennaisiin palveluihin, järjestelmiin ja infrastruktuuriin.

[3] Digitaalisen turvallisuuden arkkitehtuuri, Digi- ja väestötietovirasto 2022.



Kuva 1. Havainnointi ja reagointi osana digitaalisen turvallisuuden arkkitehtuuria

Kuvan 1 mukaisesti havainnointi ja reagointi osana digitaalisen turvallisuuden arkkitehtuuria käsittää poikkeamien havaitsemiseen, analysointiin ja käsittelyyn tarvittavat prosessit, tekniset ratkaisut ja toimintamallit sekä koko poikkeamanhallinnan elinkaaren organisoinnin. Lisäksi valvonnan tuottaman uhkatiedon jakaminen, siihen liittyvä koordinaatio ja poikkeamista viestintä ovat olennaisia havainnointiin ja reagointiin liittyviä toimintoja.

Keskeisenä tekijänä poikkeamien havaitsemisessa ovat tilannekuvan muodostamiseen erikoistuneet tietoturvavalvomotoiminnot, joiden toimintamalleja ja käyttöä kuntasektorilla tämä selvitys avaa.

2.4 Lainsäädäntö

Laki julkisen hallinnon tiedonhallinnasta

Laki julkisen hallinnon tiedonhallinnasta (ns. tiedonhallintalaki) velvoittaa julkisen hallinnon tiedonhallintayksiköitä toteuttamaan tietyt tietoturvallisuustoimenpiteet[4]. Laki velvoittaa muun muassa tapauskohtaisen järjestelmälokien keräämisen, joka toimii pohjana tietoturvavalvomotoiminnalle. Tiedonhallintalaissa säädetään lisäksi lukuisista muista tietoturvallisuusvelvoitteista, joiden toteuttamista edistää tiedonhallintalautakunta.

[4] Laki julkisen hallinnon tiedonhallinnasta. 906/9.8.2019.

Julkisen hallinnon tiedonhallintalautakunta on monialaiseen asiantuntijayhteistyöhön perustuva viranomainen, joka toimii valtiovarainministeriön yhteydessä. Valtioneuvosto nimittää tiedonhallintalautakunnan neljäksi vuodeksi kerrallaan. Tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista. [5]

Euroopan unionin kyberturvallisuuteen ja tietoturvan valvontaan liittyvä lainsäädäntö

Euroopan unionissa on meneillään useita samanaikaisia lainsäädäntöhankkeita kyberturvallisuuden parantamiseksi. Näistä tietoturvavalvomotoiminnan kannalta olennaisimpia ovat uusi kyberturvallisuusdirektiivi (ns. NIS2-direktiivi) sekä asetusluonnos kybersolidaarisuudesta.

Euroopan unionin uusi kyberturvallisuusdirektiivi yhdenmukaistaa tiettyjen yhteiskunnan kannalta kriittisten sektoreiden vähimmäistason kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden osalta. Velvoitteet vastaavat muuttuneeseen kybertoimintaympäristöön.[6]

Automaatioon pohjautuvien tai miehitettyjen tietoturvavalvomoiden hyödyntäminen helpottaa merkittävästi kyberturvallisuuspoikkeamien havaitsemista ja siten direktiivissä säädettyjen raportointivelvoitteiden täyttämistä. Määräaika direktiivin saattamiseksi osallista kansallista lainsäädäntöä on 17.10.2024 mennessä ja täytäntöönpanoa koskevien säännösten soveltaminen alkaa 18.10.2024. [7]

Tietoturvavalvomon toiminnassa on huomioitava myös henkilötiedoiksi luokiteltavien tietojen käsittely. Henkilötietojen käsittelystä säädetään Euroopan Unionin yleisessä tietosuoja-asetuksessa (*engl. GDPR, General Data Protection Regulation*). [8]

Kirjoitushetkellä lainsäädäntövaiheessa on asetusehdotus toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten. (ns. Kybersolidaarisuussäädös). [9]

Ehdotus pitää sisällään säädöksen yleiseurooppalaisesta turvaoperaatiokeskusinfrastruktuurista (ns. kyberturvallisuuden eurooppalainen suojakilpi), joka tarkoittaa käytännössä Euroopan laajuista verkostoa kansallisista ja yli rajojen toimivista kyberturvallisuuden operaatiokeskuksia (engl. *cross-border SOCs*). Ehdotuksessa kybersolidaarisuus ulottuu uhka-, havainto- ja poikkeamatietojen jakamisen lisäksi vakavien kyberhyökkäysten kohdalla avunantoon yli jäsenmaiden rajojen. Avunantoa varten ehdotetaan perustettavaksi Euroopan Unionin tasolla kyberturvallisuusreservi, joka koostuisi yksityisen sektorin tietoturvapalveluntarjoajien palveluista.

[5] Tiedonhallintalautakunta, Valtiovarainministeriö.
[6] Kyberturvallisuusdirektiivi, Euroopan parlamentti ja neuvosto 2022.
[7] Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä, LVM044:00/2022.
[8] Yleinen tietosuoja-asetus, Euroopan parlamentti ja neuvosto 2016.
[9] Kybersolidaarisuussäädös, Euroopan parlamentti ja neuvosto 2023.

Vaikka kybersolidaarisuussäädös voi vielä muuttua normaalin lainsäädäntöprosessin aikana, on oleellista seurata asetuksen lainsäädäntötyön etenemistä ja ottaa sen vaatimukset tulevaisuuden ratkaisuja harkittaessa huomioon.

3 Tietoturvavalvomo toimintona

Tietoturvavalvomo eli *Security Operations Centre* (*SOC*) muodostaa keskeisen komponentin organisaation kyvyssä valvoa digitaalista turvallisuutta ja reagoida siinä tapahtuviin poikkeamiin, aiheutuivatpa poikkeamat sitten organisaation ulkopuolisesta tai sen sisäpuolisesta syystä.

Tietoturvavalvomo kerää ja käsittelee tauotta tietoa valvottavista järjestelmistä. Tietoa toimittaviin järjestelmiin lukeutuvat esimerkiksi palomuurit, haavoittuvuuksien seurantajärjestelmät, tunkeutumisen havainnointijärjestelmät sekä verkkotasolla että yksittäisissä päätelaitteissa, automatisoidut tunkeutumisen estojärjestelmät, lokijärjestelmät ja haittaohjelmasuojaukset.

Tietoturvavalvomotoiminnan tavoitteena on havaita todennäköiset tietoturvapoikkeamat, analysoida havainnot, poistaa havaitut haittaohjelmat tai hyökkääjät ja palauttaa valvottavat järjestelmät tietoturvalliseen tilaan.

Kuva 3. Tietoturvavalvomo koostuu useasta eri osa-alueesta

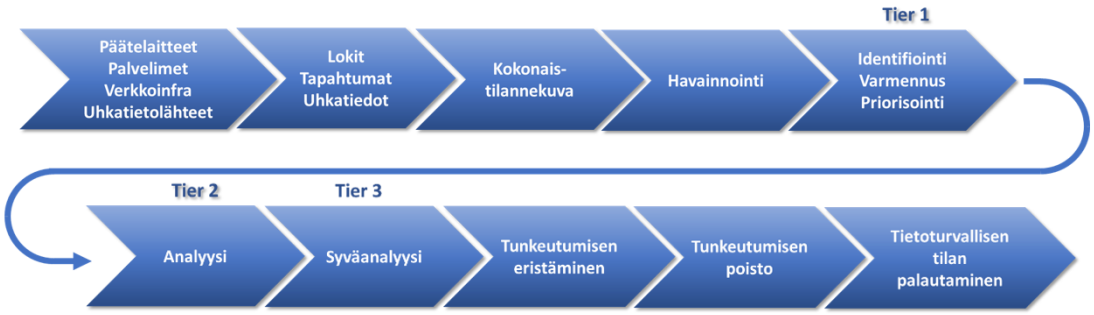
Tietoturvavalvomo sisältää lähes poikkeuksetta sekä toimintaan tarvittavan henkilöstön että teknologian, mukaan lukien keskitetyn tietoturvatiedon ja tapahtumienhallintajärjestelmän (engl. *SIEM, Security Information and Event Management*), joka auttaa ylläpitämään ajantasaista, yhtenäistä tilannekuvaa valvottavien järjestelmien kokonaistilanteesta. Nykyaikainen tietoturvavalvomo sisältää myös *SOAR*-järjestelmän *(*engl*. Security Orchestration, Automation and Response*), jolla integroidaan valvomotoiminnossa käytettäviä työkaluja ja automatisoidaan rutiininomaisia toimenpiteitä. Tietoturvatapahtumien analysointiin, priorisointiin ja suoritettaviin toimenpiteisiin SOAR-järjestelmä hyödyntää tekoälyä ja koneoppimista yhdessä tilannekohtaisen, etukäteen valmistellun toimintaohjeistuksen, eli niin sanotun pelikirjan kanssa. Ohjeistus sisältää myös tarvittaessa tilanteen ohjaamisen ihmisen käsiteltäväksi.

Tietoturvavalvomotoiminto voi olla joko organisaation sisäisesti järjestämä, ulkoisesti hankkima palvelu tai yhdistelmä eri tuotantotapoja siten, että jokin tietty osa-alue tietoturvavalvomosta on ulkoistettu ja muut toiminnot järjestetään organisaation sisäisesti.

3.1 Tietoturvavalvomon määritelmä

Tietoturvavalvomosta ei ole tietoturva-alan keskuudessa vain yhtä käsitystä tai määritelmää. Erilaisten järjestelmien ja palveluiden kirjo on laaja. Yksinkertaisimmillaan kyse on pitkälti automatisoidusta valvonnasta, jonka avulla tiedotetaan valvottavissa järjestelmissä havaitut tärkeimmät tietoturvapoikkeamat organisaation omaa jatkotarkastelua ja toimenpiteitä varten. Parhaimmillaan kyse on jatkuvatoimisesta, ympärivuorokautisesta tietoturvauhkien valvonnasta, hyökkääjien aktiivisesta jäljittämisestä kokeneiden analyytikoiden voimin sekä löydettyjen hyökkääjien nopeasta eristämisestä, poistamisesta ja järjestelmien palauttamisesta tietoturvalliseen tilaan.

Laaja-alaisen tietoturvavalvomotoiminnon keskeinen arvovirta on kuvattu kuvassa 3.



Kuva 2. Tietoturvavalvomon keskeinen arvovirta

Havainnointi ja analyysi

Tietoturvavalvomon keskiössä on aktiivinen tietoturvapoikkeamien havainnointi- ja raportointikyvykkyys. Jotta tietoturvavalvomon on mahdollista havainnoida tilannetta ja poimia mahdollisesti uhkaavia poikkeamia, sillä on oltava ajantasainen tilannekuva ja riittävä näkyvyys valvottavien järjestelmien toimintaan.

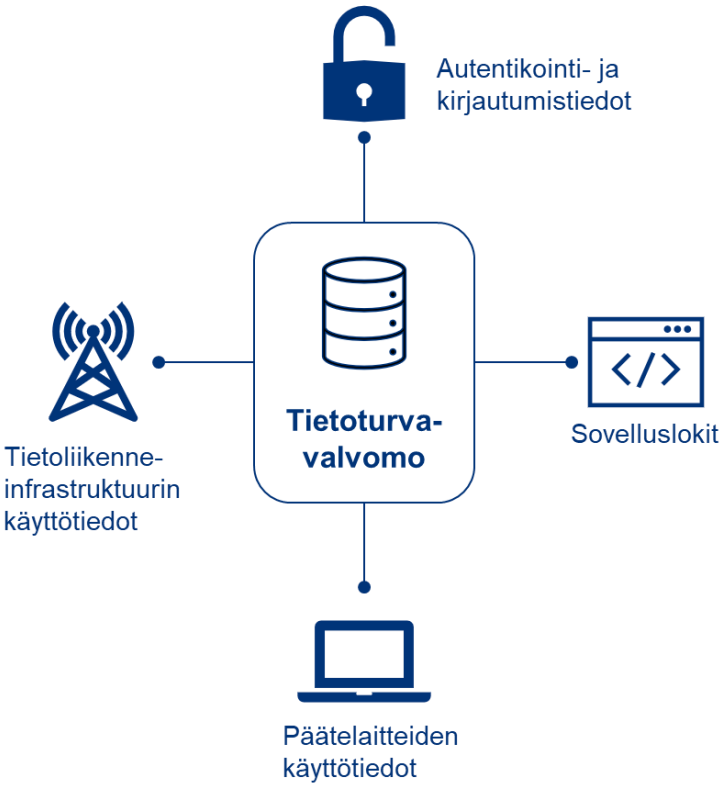
Tilannekuvan osalta uhkamaisemaa, uhkakuvia sekä tietoturvapoikkeamiin liittyviä vaarantumisen indikaattoreita pidetään keskitetysti ajan tasalla. Uhkatiedon ja indikaattorien siirtoon on määritelty omat standardoidut rakenteensa ja tiedonsiirtotapansa, joilla uhkatietoja ja indikaattoreita voidaan jakaa luotettujen tahojen kesken ja ottaa automatisoidusti käyttöön tietoturvavalvomossa. Tietoa ajankohtaisista uhista ja hyökkäyksistä sekä vaarantumisen indikaattoreita käytetään aktiiviseen havainnointiin sekä havaintojen tulkitsemiseen ja niiden vakavuuden arviointiin.

Tapahtumatietoa puolestaan kerätään tietojenkäsittely-ympäristöjen suojaamiseen ja tarkkailuun käytettävistä ohjelmistoista, kuten esimerkiksi päätelaitesuojauksesta, palomuureista, sekä järjestelmä-, sovellus- ja tietoliikennelokeista. Tapahtumatietolähteiden liittäminen tietoturvavalvomon havainnointiverkkoon on osa kattavaa tietoturvavalvomopalvelua.

Lisänäkyvyyttä havainnoitaviin järjestelmiin saadaan asentamalla erityisiä valvontaohjelmistoja (*sensoreita*) palvelimiin, verkkolaitteisiin ja käyttäjien työasemiin. Esimerkiksi päätelaitteisiin ja palvelinalustoille asennettavat, kehittyneet EDR- ja XDR-ohjelmistot (engl. *Endpoint Detection and Response, Extended Detection and Response*) tarjoavat perinteisen tapahtumatiedon keräämisen lisäksi usein myös hyvän jäljitettävyyden työaseman viimeaikaisiin tapahtumiin. Lisäksi näiden ohjelmistojen avulla tietoturvapoikkeamatilanteissa voidaan toteuttaa etukäteen määriteltyihin käytänteisiin perustuvia automaattisia reagoinnin toimenpiteitä. Valvontaohjelmistot pystyvät parhaimmillaan näyttämään aikajanalla koko tietoturvapoikkeamaan liittyvän tapahtumaketjun ja suorittamaan poikkeamalle automatisoidun juurisyyanalyysin. Tämä helpottaa ja nopeuttaa poikkeaman vaarallisuuden tai vaarattomuuden arviointia sekä auttaa ymmärtämään tapaa, jolla hyökkääjä toimii.

Uhkia aktiivisesti ja kehittyneesti tarkkailevia ohjelmistoja voidaan asentaa päätelaitteiden lisäksi palvelimiin ja verkkoinfrastruktuurilaitteisiin. Kattavassa tietoturvavalvomokokonaisuudessa tarvittavien ohjelmistojen lisenssit, asennus ja ylläpito kuuluvat palveluun.

Kun koko valvottavan järjestelmäkokonaisuuden tapahtumatiedot päätelaitteista, palvelimista ja verkkolaitteista keskitetään yhteen paikkaan, tyypillisesti *SIEM*-järjestelmään, on mahdollista korreloida tapahtumia koko valvottavan tietojenkäsittely-ympäristön laajuisesti. Tällöin on mahdollista havaita hyökkäyksiä helpommin ja nopeammin.



Kuva 3. Tietoturvavalvomo kerää ympäristön havainnointitietoja ja reagoi poikkeamiin

Edistyneimmillään havainnointia voidaan tukea etsimällä aktiivisesti hyökkääjien jälkiä käytössä olevista järjestelmistä siihen erikoistuneiden tietoturva-asiantuntijoiden voimin (engl. *threat hunting*). Tällöin on mahdollista havaita myös sellaisia viitteitä hyökkäyksistä, joita tietoturvavalvomon automatisoidut havainnointi- ja hälytysjärjestelmät eivät osaa valikoida jatkotutkinnan kohteiksi riittävän korkealla prioriteetilla.

Oleellinen osa oikean havainnointikyvyn rakentamista on koko tietojenkäsittely-ympäristön normaalitilan ymmärrys, mukaan lukien sellaiset normaalit tilanteet ja tapahtumat, jotka herättävät tietoturvavalvomon huomion. Näkemys tästä päivittyy tietoturvavalvomon toiminnan aikana, sillä organisaation tietotekninen infrastruktuuri on tyypillisesti jatkuvan muutoksen tilassa. Normaalitilan tunnistaminen mahdollistaa järjestelmän suodattimien päivityksen, joka vähentää turhia hälytyksiä ja lisää kykyä keskittyä todellisiin uhkiin.

Reagointi ja suojaustoimenpiteet

Suurin osa tietoturvavalvomoista käsittää valvonnan lisäksi myös tietoturvapoikkeamiin reagoinnin, joka voi olla esimerkiksi tunnistetun haittaohjelman eristämistä ja poistamista, järjestelmissä havaittujen tunkeutujien poistoa ja valvottavien järjestelmien tietoturvallisen tilan palautusta. Tietoturvavalvomon hyödyt jäävätkin kovin vähäisiksi, mikäli valvontaan ei liity kykyä reagoida havaittuihin poikkeamiin riittävän nopeasti, sillä erityisesti kohdennetut hyökkäykset voivat alkaa yllättäen ja olla varsin nopeasti ohitse.

Tietoturvan suojausmekanismien rakentaminen ei yleisen käsityksen mukaan kuulu suoranaisesti tietoturvavalvomotoiminnon piiriin, mutta valvomo pystyy täydentämään ja vahvistamaan suojaustoimenpiteitä tietyissä tilanteissa. Esimerkiksi palomuurien konfiguraatioita voidaan muuttaa ajantasaisen uhkatiedon perusteella siten, että kansainvälisesti tietoverkoissa havaitut uudet automatisoidut hyökkäykset saadaan estettyä ennen kuin ne pääsevät organisaation järjestelmiin. Lisäksi tapahtuneiden tietoturvaloukkausten osalta voidaan analysoida hyökkäyksen mahdollistaneet olosuhteet ja toteuttaa muutoksia, joilla vastaavat hyökkäykset estetään jatkossa.

Joissain tapauksissa tietoturvavalvomon toimintoihin kuuluu myös tietojärjestelmien jatkuvatoiminen, aktiivinen tarkistaminen tunnettujen ohjelmistohaavoittuvuuksien ja konfiguraatiovirheiden löytämiseksi (engl. *vulnerability scanning)*.

Tietoturvavalvomo ja pilvipalvelut

Pilvipalvelupohjaiset ratkaisut ovat keskeinen osa nykyaikaisia tietojenkäsittely-ympäristöjä. Tietoturvavalvomon näkökulmasta yleisimpien julkisten pilvipalvelualustojen integrointi valvonnan piiriin on kohtalaisen helppoa, nopeaa ja kustannustehokasta, sillä julkiset pilvipalvelut tarjoavat useimmiten kehittyneet työkalut ja valmiit rajapinnat valvontaan.

Riippuen pilvipalvelun palvelumallista tietoturvan valvonta saattaa myös kuulu sisäänrakennettuna palveluun ja näin ollen vastuu tietoturvan valvonnasta säilyy palvelun tarjoajalla. Erityisesti ohjelmistopalveluiden (Software as a Service) osalta palvelun käyttäjän saattaa olla vaikeata saada riittävää läpinäkyvyyttä palvelun sisältämään infrastruktuuriin valvonnan toteuttamiseksi, jolloin tulisi varmistua siitä, että valvonta joko kuuluu palveluun tai palvelu tarjoaa rajapinnan tietoturvavalvomon hyödynnettäväksi.

3.2 Kustannusrakenne

Erilaisilla organisaatioilla on erilaisia tarpeita tietoturvavalvomon suhteen. Koska kysynnässä on kirjoa ja palvelun laajuus vaikuttaa merkittävästi palvelun hintatasoon, osa tietoturvavalvomopalvelun tarjoajista on ratkaissut asian tarjoamalla palveluaan useina eri laajuisina ja eri hintaisina paketteina. Tietoturvavalvomopalveluiden koostamiseen ja hinnoitteluun ei kuitenkaan ole olemassa varsinaista standardimallia. Käytännössä hinnoittelumalli perustuu usein tapaan, jolla palvelutuottaja on rakentanut palvelunsa. Hinnoittelurakenteessa tietoturvavalvomopalvelun kustannusperusteena voi olla esimerkiksi:

- käyttäjien määrä,
- työasemien määrä,
- muiden valvottavien kohteiden (palvelin, verkkolaite tms.) määrä,
- lokilähteiden kokonaismäärä,
- analysoitavien tietoturvatapahtumien määrä sekä
- palvelutaso, kattaen sekä palvelun laajuuden että sovitut vasteajat.

Organisaatio voi myös itse miehittää oman tietoturvavalvomotoimintonsa, mutta toimitiloineen, henkilöstöineen, laitteineen ja ohjelmistolisensseineen se on yleisen markkinanäkemyksen mukaan sekä kustannuksena että työnmäärällisesti moninkertainen verrattuna ulkoistetun palvelun käyttöön. Skaalaetujen vuoksi selkeästi kustannustehokkaampaa on ulkoistus useaa organisaatioita samanaikaisesti palvelevaan tietoturvavalvomoon. Vain yhtä organisaatiota palveleva tietoturvavalvomo vaatii useampaa organisaatiota palvelevan valvomon tavoin täysimittaisen, ympärivuorokautisen valmiuden poikkeamien havainnointiin ja hyökkäysten torjuntaan.

Kustannustehokkuus ja skaalautuvuus

Selvitystyön yhteydessä toteutettujen työpajojen sekä haastatteluiden perusteella tietoturvavalvomopalvelun kustannustehokkuus ja skaalautuvuus ovat keskeisiä tekijöitä palvelun käyttöönotolle kuntaorganisaatioissa.

Kustannustehokkuuteen vaikuttaa merkittävästi muun muassa

- automaation ja koneoppimisen hyödyntäminen,
- hankittavan palvelun oikeanlainen mitoitus,
- palvelukokonaisuuksien, toimittajaekosysteemien ja olemassa olevien lisenssien oikeanlainen hyödyntäminen sekä
- panostukset ympäristöjen ja infrastruktuurin suojaamiseen.

Tietoturvavalvomon kustannustehokkuuden ja skaalautuvuuden optimointi tarkoittaa ennen kaikkea ihmistyön kohdentamista tehtäviin, jossa ihmisen kyvykkyyttä nimenomaisesti tarvitaan, ja kaikkien automatisoitavissa olevien tehtävien automatisointia. Keskeisiä komponentteja tässä ovat automaation maksimointi sekä koneoppimisen ja ennalta määritellyn toimintaohjeistuksen käyttö.

Kustannustehokkuutta voi parantaa lisäksi mitoittamalla palvelu tarpeiden mukaiseksi. Tämä tapahtuu esimerkiksi rakentamalla tietoturvavalvomopalvelua asteittain ja sisällyttämällä ainakin alkuvaiheessa valvonnan piiriin vain riskiarvioinnin perusteella organisaation kannalta oleellisimmat järjestelmät ja kohteet. Myös käytössä olevien palveluiden, järjestelmien ja toimittajaekosysteemien oikeanlainen hyödyntäminen parantaa tietoturvavalvomon kustannustehokkuutta. Tiettyjen palvelukokonaisuuksien osalta lisenssi- ja käyttökustannuksiin saattaa sisältyä oletuksena tietoturvavalvomon kannalta merkittäviäkin valvontakyvykkyyksiä, jotka organisaation on osattava hyödyntää. Tietoturvan valvontaan liittyviä vaatimuksia voidaan myös sisällyttää muihin palvelusopimuksiin jo hankintavaiheessa, jolloin valvontaa ei tarvitse rakentaa jälkikäteen palvelun päälle.

Kustannustehokkuudessa auttaa luonnollisesti myös panostus riittäviin suojaamisen toimenpiteisiin, sillä jokainen suojaukseen pysähtynyt hyökkäys vähentää tietoturvavalvomon työmäärää ja siten kustannustasoa. Esimerkiksi nollaluottamusmallin (engl. *Zero Trust*) periaatteiden[10] mukainen lähestymistapa nähtiin toimivana tapana parantaa tietojenkäsittely-ympäristöjen suojausta.

[10] Digitaalisen turvallisuuden arkkitehtuuri: Nollaluottamusmallin periaatteet, Digi- ja väestötietovirasto 2022.

3.3 Tulevaisuudennäkymiä

Selvityksen yhteydessä järjestettyjen työpajojen myötä kävi selväksi, että ei ole mielekästä tukeutua aikaisempien vuosien menetelmiin ja mielikuviin paljon manuaalista työtä ja henkilöresursseja vaativista tietoturvavalvomoista, jotka pohjautuvat vahvasti keskitettyyn lokienhallintaan ja lokien säännölliseen analysointiin. Tietoturvan valvontatuotteiden teknologisen kehityksen mukanaan tuoma automaation, koneoppimisen ja tekoälyn lisääntyminen vaikuttavat merkittävästi siihen, millaisia resursseja tietoturvapoikkeamiin reagoiminen vaatii.

Esimerkiksi perinteisten SIEM-ratkaisujen hyödyllisyyden tietoturvan oikea-aikaisessa valvonnassa katsotaan laskeneen, sillä niitä on vaikea pitää ajan tasalla nykyisessä, nopeasti muuttuvassa uhkatilanteessa. Ratkaisujen pilvipohjaisuus, koneoppiminen, mahdollisten tietoturvapoikkeaminen automatisoitu analysointi ja niihin reagointi sekä uhkaluokittelu ovat tulleet perinteisten SIEM-ratkaisujen rinnalle ja ne tarjoavatkin usein toiminnallisuuksia, joita pelkkä SIEM-ratkaisu ei tarjoa. Työpajojen näkemyksen mukaan pelkkää SIEM-ratkaisua ei enää nykypäivänä kannatakaan mieltää tietoturvavalvomototeutusten keskiöön.

Yleisesti ottaen automaatio ja tekoäly ovat täysin muuttamassa sitä, miltä tietoturvavalvomo näyttää teknisestä ja operatiivisesta näkökulmasta. Automaation ja tekoälyn käyttö ennalta määritellyn toimintaohjeistuksen ja koneoppimisen kanssa tulevat valtaamaan alaa myös tietoturvan valvonnassa, mikä näkyy jo nyt positiivisesti esimerkiksi havaittujen poikkeamien käsittelyajoissa. Vähäprioriteettisten poikkeamien käsittelyajat saadaan laskettua lähelle nollaa, kun ne voidaan hoitaa välittömästi ilman ihmisen osallisuutta. Ennen vähäprioriteettisten tapausten vastinajat saattoivat olla huomattavan pitkiä niiden priorisoituessa työjonojen hännille.

Tulevaisuudessa tekoälyn ja automatisoinnin käyttöä tietoturvan valvonnassa korostaa entisestään vastaavien teknologioiden käyttö yhä enenevissä määrin myös hyökkäyksissä. Automatisoitua, älykästä konehyökkääjää vastaan manuaalityöhön perustuva valvonta ja puolustus tulee olemaan auttamattoman hidas.

Näköpiirissä oleva lähitulevaisuuden tietoturvavalvomo tulee olemaan lähes täysin automatisoidusti toimiva konejärjestelmä, joka ottaa ihmisen mukaan päätöksentekoon tilanteissa, joissa sitä sen näkemyksen mukaan tarvitaan. Asiantuntijoiden rooli tietoturvavalvomotoiminnassa tulee todennäköisesti muuttumaan kohti vaativien kokonaistilanteiden hallintaa ja koordinointia sekä kriittisten päätösten tekoa.

Yhteistyön osalta voidaan nähdä, että verkottuneisuus ja tiedonvaihto luotettujen kotimaisten ja kansainvälisten kumppaneiden kanssa tulee muodostumaan entistä tärkeämmäksi samoin kuin automatisoitu tiedonvaihto ja tiedon automaattinen käyttöönotto tietoturvavalvomoiden toiminnassa.

4 Tietoturvavalvomotoiminto kuntien näkökulmasta

Kuntien ja muun julkisen hallinnon kansalaisille tarjoamat palvelut ovat digitalisaation myötä siirtyneet yhä enenevässä määrin käytettäväksi tietoverkkojen välityksellä päätelaitteesta, ajasta ja paikasta riippumatta. Kansalaisten tietoja myös käsitellään erilaisissa tietojärjestelmissä ja tietovarannoissa, jotta tarjotut palvelut olisivat mahdollisimman sujuvia.

Tästä syystä myös kuntien, kuten kaikkien digitaalisessa toimintaympäristössä toimivien toimijoiden, on tarpeen panostaa digitaaliseen turvallisuuteen. Nykypäivänä mikään organisaatio ei voi enää suhtautua tietoverkkojen ja digitaalisten palveluiden turvallisuuteen itsestäänselvyytenä. Digitaaliseen turvallisuuteen tulee panostaa kokonaisvaltaisesti ja sitä tulee kehittää jatkuvasti sitä mukaan, kun erilaiset digitaalisiin palveluihin kohdistuvat hyökkäysmenetelmät kehittyvät ja monipuolistuvat.

Tietoturvavalvomo on vain yksi, mutta huomattavan tärkeä osa digitaalisen turvallisuuden arkkitehtuuria. Tietoturvavalvomo tuo organisaatiolle näkyvyyden muutoin melko hankalastikin tarkkailtaviin tietoverkkoihin ja digitaaliseen ympäristöön.

4.1 Kunnista ja tietohallinnon järjestämisestä yleisesti

Suomessa on vuonna 2023 yhteensä 309 kuntaa, joiden koko vaihtelee hieman yli 100 asukkaan kunnasta yli 650 000 asukkaan kuntaan. Kuntaliiton vuonna 2022 tekemän ”*Kuntien tietohallinnon roolit*” -selvityksen mukaan kuntien tietohallinto on monimuotoista ja käytössä on erittäin laaja skaala erilaisia tietoteknisiä ratkaisuja.

Kuntaliiton selvityksen mukaan kuntien ICT-toiminteen mahdollisia järjestämismalleja voivat olla esim.

- palvelun itse järjestäminen ja tuottaminen,
- inhouse-yhtiön käyttäminen,
- isäntäkuntamalli sekä
- ulkoistaminen yksityisiä palvelutoimittajia hyödyntäen.

Usein tietohallinnon palveluiden järjestäminen kunnissa on kokoelma erilaisia järjestämismalleja, joihin liittyy vaihtelevia yhteistyötapoja ja käytäntöjä. Kuntien toimintaympäristö ja tehtäväkenttä on hyvin moniulotteinen, eikä ehdoton yhteen järjestämismalliin pyrkinen ole Kuntaliiton selvityksen mukaan realistinen päämäärä.[11]

4.2 Tietoturvavalvomoiden nykytila kunnissa

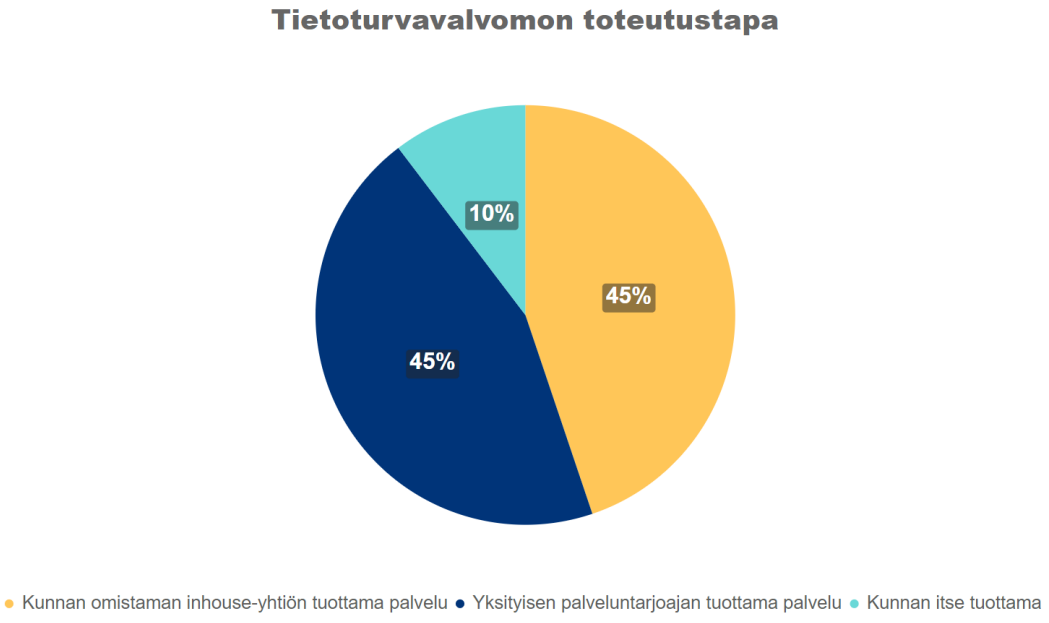
Kuntien tietoturvavalvomoiden käytön nykytilaa selvitettiin kaikille Suomen kunnille lähetyn verkkokyselylomakkeen sekä kuudelle eri kokoiselle kunnalle kohdennetun teemahaastattelun avulla. Kyselyn ja teemahaastattelujen tulokset esitellään yleisellä tasolla tässä kappaleessa.

[11] Kuntien tietohallinnon roolit, Kuntaliitto 2022

Kyselylinkki toimitettiin kaikille kunnille sähköpostitse kirjaamojakeluna. Kyselylinkin saatteessa ohjeistettiin kirjaamoita toimittamaan kysely kunnan tietoturvallisuudesta vastaavalle taholle. Kyselyyn vastasi määräaikaan mennessä yhteensä 119 kuntaa yhteensä 309 kunnasta, joten vastausprosentiksi muodostui noin 39 %. Tilastoja tulkittaessa on hyvä ottaa huomioon, että vastaamatta jättäneet kunnat ovat todennäköisemmin niitä, joissa tietoturvallisuudesta vastaavaa tahoa ei tunnistettu tai sitä ei ole resursoitu. Vastaajien hajauma niin maantieteellisesti kuin kunnan kokoluokan perusteella on kuitenkin varsin kattava, joten tuloksia voidaan pitää varsin luotettavina.

4.2.1 Kuntien tietoturvavalvomon toteutustapa vaihtelee

Niillä kunnilla, joilla tietoturvavalvomo oli käytössään, valvomoiden järjestelytavat jakautuivat kuntien itse tuottamiin valvomoihin sekä kuntaomisteisten inhouse-yhtiöiden ja yksityisten palveluntarjoajien tuottamiin tietoturvavalvomopalveluihin (kuva 5). Noin 10 % tietoturvavalvomoista oli kuntien itse tuottamia, 45 % vastauksen jättäneistä kunnista hyödyntää omistamansa inhouse-yhtiöiden tuottamia tietoturvavalvomopalveluita ja niin ikään 45 % kunnista hyödyntää yksityisten palveluntarjoajien valvomopalveluita. Tämän lisäksi osalla kunnista tietoturvan valvonta saattaa sisältyä pistemäisenä myös tiettyihin ratkaisukokonaisuuksiin, kuten esimerkiksi pilvipalveluna hankittuihin ohjelmistoihin, mutta tällaisessa tapauksessa ei voida puhua täysimittaisesta tietoturvavalvomotoiminnosta.



Kuva 4. Tietoturvavalvomon toteutustapa

Sekä kunnille toteutetuissa haastatteluissa, että kyselyn vastauksissa kävi ilmi, että tietoturvavalvomotoiminne on usein hankittu samalta palveluntarjoajalta, joka tuottaa kunnalle tietohallinnon peruspalvelut kuten kapasiteetin, työympäristön ja päätelaitteiden hallinnan tai verkkopalvelut. Tietoturvavalvomopalveluiden tuottaminen infrastruktuuripalveluiden kanssa rinnakkain saattaakin useissa tapauksissa edistää palvelutuotannon kustannustehokkuutta, muun muassa teknologialisenssien ja palvelutuotannossa tehdyn työn osalta.

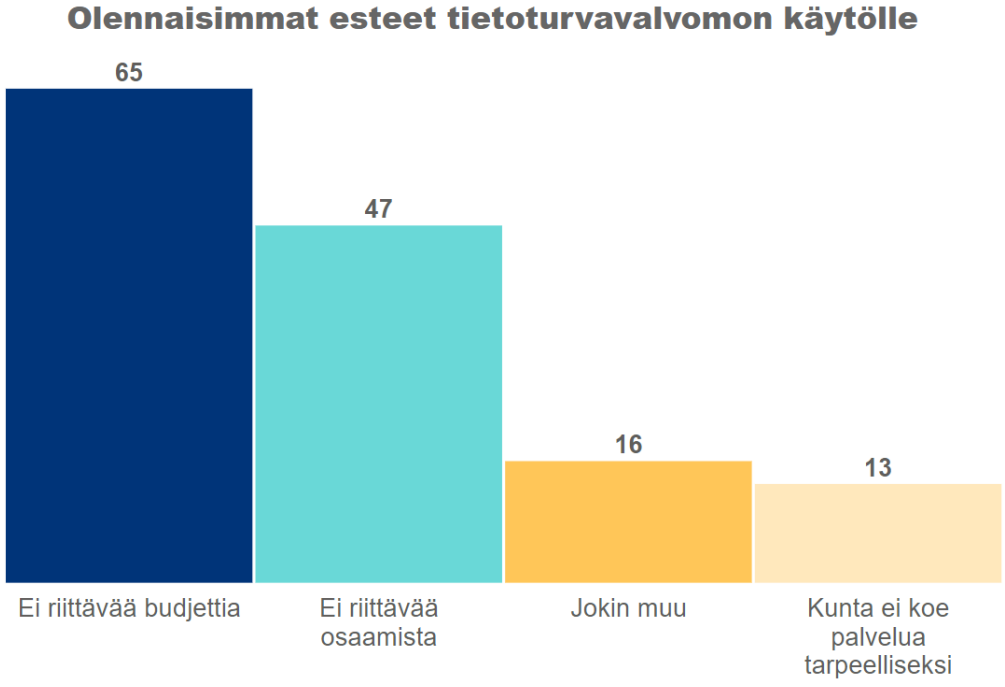
4.3 Yleisimmät esteet tietoturvavalvomon käytölle kunnissa

Selvityksessä tiedusteltiin myös olennaisimpia esteitä tietoturvavalvomon käyttöönotolle ja hyödyntämiselle niissä kunnissa, joilla tietoturvavalvomoa ei ollut käytössään.

Haastatellut kuntaorganisaatiot kokivat haasteeksi ennen kaikkea sen, että tietoturvavalvomon ollessa uusi, pysyvä toiminto, se tarvitsee vastaavasti pysyvän resurssoinnin ja rahoituksen. Kuntien tietohallinnossa tietoturvavalvomon hyödyllisyyttä ja tarpeellisuutta ei useinkaan kyseenalaistettu, vaan tietoturvavalvomoiden käyttöönottoon suhtauduttiin positiivisesti. Valtaosa kuntaorganisaatioista ottaisi tietoturvavalvomon käyttöön, jos siihen olisi helppo ja kustannustasoltaan riittävän edullinen tapa.

Valtaosa verkkokyselyyn vastaajista mainitsi olennaisimmiksi esteiksi nimenomaan budjetin riittämättömyyden tai tietoturvavalvomoiden käyttöönottoon liittyvän osaamisen puutteen. Haastatteluja myötäillen vain kohtalaisen harva kyselyyn vastannut kunta katsoi, ettei tietoturvavalvomo ollut tarpeellinen heidän toimintansa kannalta.

Erityisesti pienempien kuntien osalta tietoturvavalvomon aiheuttamat kustannukset katsottiin liian korkeiksi tietohallinnon käytössä oleviin taloudellisiin ja henkilöstöresursseihin nähden. Kuvassa 6 on jaoteltu olennaisimmat esteet tietoturvavalvomon käytölle kyselyn vastausmäärien mukaisesti.



Kuva 5. Olennaisimmat esteet tietoturvavalvomon käytölle

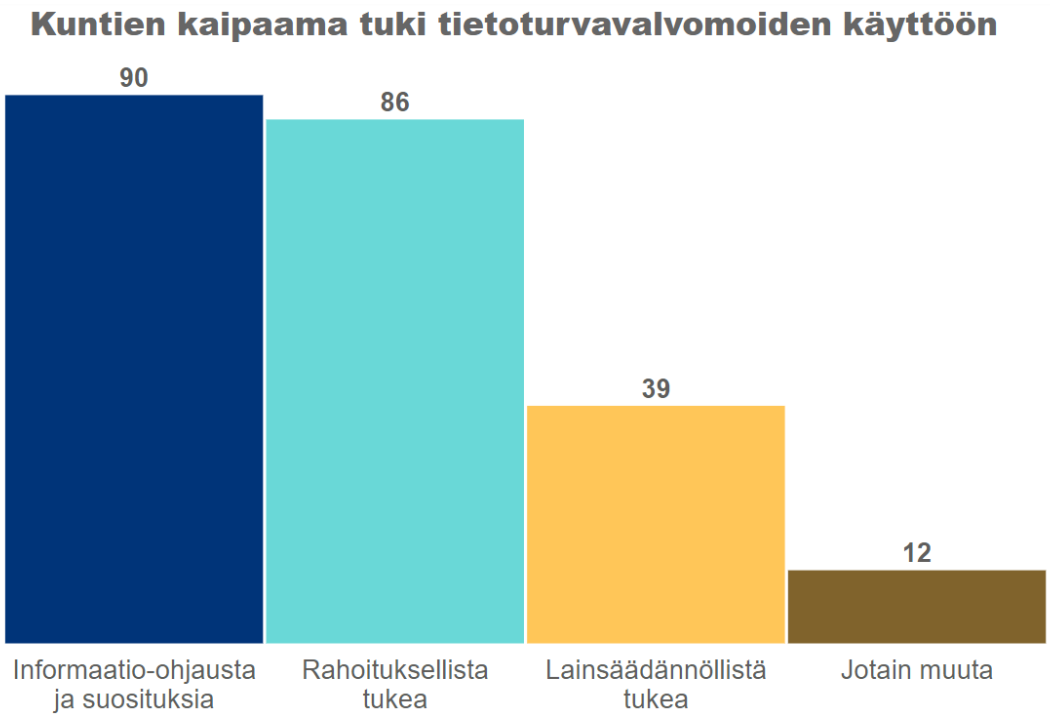
Kyselyn avoimista vastauksista kuitenkin selviää, että esteet tietoturvavalvomon käyttöönotolle ovat huomattavasti moninaisemmat kuin vain osaamisen ja budjetin riittämättömyys. Muutamassa vastauksessa ilmeni muun muassa hyvinvointialueiden aloitus ja kunnan näkökulmasta kaikkein kriittisimpien järjestelmien siirtyminen

hyvinvointialueiden ylläpidettäväksi. Tällaisessa tapauksessa kunnassa ei välttämättä kyetä perustelemaan investointia tietoturvavalvomotoimintaan riskiperusteisesti. Huomattavaa kuitenkin on, että hyvinvointialueuudistuksenkin jälkeen kunnille jää merkittäviä salassa pidettävää henkilötietoa sisältäviä järjestelmiä, muun muassa varhaiskasvatuksen ja sivistystoimen toimialoilla.

Lisäksi esteinä tietoturvavalvomon käytölle nousivat riittävän hankintaosaamisen puute, tietoturvatuotteiden ja -palveluiden markkinatuntemuksen puute sekä puutteet tietoturvan perusasioissa. Osa vastaajista näkee tietoturvavalvomon edistyksellisen tason toimintona, joka on järkevää ottaa käyttöön vasta kun digitaalisen turvallisuuden perusteet, kuten esimerkiksi riskienhallinta ja poikkeamanhallinta on toteutettu riittävän hyvin. Esimerkiksi laajat puutteet poikkeamanhallinnan prosesseissa saattavat tehdä valvonnasta melko hyödytöntä, mikäli havaittuihin tietoturvan poikkeamiin reagointi ei ole mahdollista.

4.3.1 Kuntien kaipaama tuki tietoturvavalvomoiden käyttöön

Selvityksen yhteydessä toteutetun verkkokyselyn ja haastattelujen perusteella kunnat kaipaavat erityisesti keskitettyä, viranomaislähtöistä informaatio-ohjausta ja suosituksia sekä rahoituksellista tukea tietoturvavalvomoiden laajempaan hyödyntämiseen. Kuvassa 7 esitetään vastausmäärien mukaisesti, millaista tukea kunnat kaipaavat tietoturvavalvomoiden käyttöön.



Kuva 6. Millaista tukea tietoturvavalvomoiden käyttöön kaivataan kunnissa?

Avointen vastausten ja haastattelujen perusteella kuntien tietohallinnoissa on vahva ymmärrys tietoturvavalvomoiden tarpeellisuudesta ja hyödyistä, mutta hyötyjen kommunikointi ylimmälle johdolle ja taloudellisten päätösten tekijöille on paikoin ollut haastavaa. Näin ollen julkisen hallinnon digitaalisen turvallisuuden kentällä toimivien viranomaisten laatimat ohjeistukset ja painokkaatkin suositukset koettiin yhtenä keskeisenä keinona helpottaa tietoturvavalvomotoiminnan kehittymistä kunnissa.

Tämän lisäksi konkreettisina ehdotuksina tietoturvavalvomoiden käytön tukemiselle nostettiin muun muassa usean eri kunnan tekemät yhteishankinnat ja näin saavutettu skaalaetu, kilpailutusten ja hankintaosaamisen keskitetty tukeminen sekä taloudelliset kannustimet esimerkiksi käyttöönotto- tai pilotointivaiheessa.

Sen sijaan velvoittavat määräykset ja lainsäädäntö jakoivat vastaajien mielipiteitä vahvasti, sillä toisaalta velvoitteiden koettiin helpottavan tietoturvavalvomoiden aiheuttamien kustannusten perustelemista, mutta toisaalta osalla kunnista on jo nyt vaikeuksia täyttää tiedonhallinnalle ja tietoturvallisuudelle asetettuja lainsäädännöllisiä velvoitteita. Osa vastaajista näki myös tietosuojaan liittyvät kysymykset ongelmallisina, sillä tietoturvapoikkeamien selvittelyssä joudutaan usein käsittelemään yksityiskohtaisella tasolla tietojärjestelmissä olevaa tietoa, joka saattaa sisältää myös henkilötiedoksi luokiteltavaa tietoa. Laajamittaisessa raportoinnissa saattaa tämän myötä helposti syntyä myös kasaumavaikutuksia. Yleisen käsityksen mukaan kuntien näkökulmasta selkeitä vaatimuksia on hyvä asettaa, mutta vain siten, että ne pystytään toteuttamaan järkevästi.

Valtakunnallisesti keskitetyn tietoturvavalvomon käytölle nähtiin erityisesti teknisluonteisia haasteita kuntien tietojenkäsittely-ympäristöjen monimuotoisuuden takia, sillä ainakin osa kunnista kaipaa erityisesti omaan ympäristöönsä sopivia ja räätälöitäviä palveluita. Kuntien itsenäisyys päätöksenteossa asettaa lisäksi omat haasteensa valtakunnalliselle, yhtenäisesti toimivalle tietoturvan valvonnalle. Sen sijaan ajatus alueellisista tietoturvavalvomoista sai varovaista kannatusta, sillä osalla hyvinvointialueista ja alueella sijaitsevilla kunnilla on joka tapauksessa palvelutuotannossaan tiivistä yhteistyötä.

Yhtenä jatkokehitysmahdollisuutena nähtiin julkishallinnon yhteishankintayksikkö Hanselin kautta tehty kilpailutus, jota kunnat voisivat hyödyntää tietoturvavalvomopalvelua hankkiessaan. Kilpailutuksessa tulisi kuitenkin ottaa huomioon, että kuntien tarpeet valvonnan laajuudelle vaihtelevat.

4.4 Kunnan valmiudet edesauttavat tietoturvavalvomon onnistumisessa

Tietoturvavalvomopalveluita tarjoavien palveluntarjoajien kokemusten pohjalta on selvää, että ulkoistettuakaan tietoturvavalvomoa ei ole mahdollista ottaa käyttöön ilman tiettyjä kyvykkyyksiä valvottavan ympäristön omistavassa asiakasorganisaatiossa. Tyypillinen ongelma tietoturvavalvomon käyttöönoton yhteydessä on tarkan tiedon puute valvottavista kohteista, niiden sisältämistä toiminnallisuuksista ja kriittisestä tiedosta. Toinen usein toistuva haaste on asiakasorganisaation puutteellinen kyvykkyys tukea valvomotoimintaa kriittisissä tilanteissa.

Palveluntarjoajien kokemusten mukaan organisaation valmiuteen vaikuttavat postitiivisesti etenkin organisaatiossa käyttöön otetut, tunnetut standardit ja sertifioinnit digitaalisen turvallisuuden eri osa-alueilla. Hyvänä viitekehyksenä digitaalisen turvallisuuden kokonaisuuden rakentamiseen mainittiin muun muassa yhdysvaltalaisen *National*

Institute of Standards and Technologyn (NIST) laatima *Cybersecurity Framework*, johon myös Digi- ja väestötietoviraston julkaisema digitaalisen turvallisuuden arkkitehtuurimalli perustuu.

Ajantasainen kuva valvottavasta ympäristöstä

Tietoturvavalvomon kannalta optimaalisen tilannekuvan ylläpito valvottavista kohteista vaatii tietoa, joka syntyy organisaation toteuttaessa säännöllisesti ja toistuvasti toiminnan, tiedon ja ympäristöjen kriittisyysluokittelua, jatkuvuussuunnittelua ja riskiarviointeja. Laajamittaiseen valvottavien kohteiden kartoittamiseen liittyy merkittäviä haasteita, sillä nykyaikaisissa tietojenkäsittely-ympäristöissä tieto jakautuu ja monistuu useisiin kohteisiin erilaisten tuotantotapojen, alustojen ja varajärjestelmien myötä.

Yleisesti ottaen tiedon puute valvottavasta infrastruktuurista aiheuttaa tehottomuutta tietoturvan valvonnassa, vähentää havainnointi-, reagointikyvykkyyttä sekä lisää riskiä tietoturvapoikkeamien yhteydessä organisaatiolle tapahtuvista vahingoista. Ilman ajantasaista tietoa valvottavasta ympäristöstä tietoturvavalvomo ei pysty kohdentamaan valvontaa kriittisimpiin järjestelmiin eikä priorisoimaan mahdollisten turvallisuusloukkauksien käsittelyä.

Toimivaltuudet ja roolit poikkeamatilanteessa

Järjestämis- ja tuotantotavasta riippumatta tietoturvavalvomo tarvitsee mahdollisimman selkeän prosessin siihen, miten valvomo ottaa tarvittaessa yhteyttä kuntaan sekä siihen, miten valvomo saa tarvittaessa kunnalta riittävää päätöksentekotukea toimiakseen tehokkaasti poikkeamatilanteissa. Prosessissa on huomioitava, että tietoturvavalvomo toimii usein ympärivuokokautisesti ja hyökkäyksiä voi esiintyä milloin tahansa, joten päätöksentekoon on kyettävä myös tavanomaisten työskentelyaikojen ulkopuolella. Ennalta määritetyt ja selkeästi sovitut toimintavaltuudet eri sidosryhmien välillä helpottavat huomattavasti toimintaa poikkeamatilanteessa.

Työpajoissa esitetty näkemys oli, että poikkeamatilanteessa tietoturvavalvomon suorittaman ensivasteen nopeus on keskeinen tekijä tietoturvahyökkäysten torjunnassa, ja sen vuoksi tietoturvavalvomo kannattaakin valtuuttaa toteutustavasta riippumatta toimimaan mahdollisimman laajasti. Käytännön työssä varsin heikkojenkin signaalien perusteella on pystytty estämään isoja poikkeamia, jos tietoturvavalvomon toimintavaltuudet ovat olleet kunnossa. On kuitenkin hyvä huomata, että kriittistä päätöksentekoa on mahdotonta ulkoistaa täydessä mittakaavassa ja vastuu kuntalaisten julkisten palveluiden saatavuudesta ja toimivuudesta, tietosuojasta ja -turvasta sijaitsee kuitenkin viime kädessä kunnalla itsellään.

5 Kuntien tietoturvavalvomoiden vaihtoehtoiset järjestämistavat

Kuten edellä olevista tietoturvavalvomoa toimintona käsittelevistä kappaleista käy ilmi, toiminnan järjestämiseen on useita vaihtoehtoisia tapoja ja tietoturvavalvomo itsessään voi pitää sisällään varsin vaihtelevissa määrin erilaisia digitaalisen turvallisuuden havainnointiin ja reagointiin liittyviä toimintoja. Tässä selvityksessä ei käsitellä tietoturvavalvomon ratkaisu- tai toteutusvaihtoehtoja yksittäisen kunnan näkökulmasta vaan eri järjestämistapoja tarkastellaan mahdollisimman laajasti koko kuntatoimialan näkökulmasta.

5.1 Keskitetty tietoturvavalvomo kuntatoimialalle

Kansallisella, kuntien keskitetyllä tietoturvavalvomolla tarkoitetaan tässä yhteydessä erikseen perustettavaa tietoturvavalvomo-organisaatiota, joka palvelisi kaikkia kuntia. Se toimisi itsenäisesti sisältäen valvontaan tarvittavat henkilöresurssit, teknologiat ja hallinnon. Tietoturvavalvomo voisi tällaisessa tapauksessa toimia joko keskitetyn rahoituksen turvin tai asiakasrahoitteisesti, jolloin jokainen palvelua hyödyntävä kunta osallistuisi valvomon kustannuksiin palvelun hinnoittelumallin mukaisesti.

Kuva 7. Keskitetty tietoturvavalvomo

Keskitetyn tietoturvavalvomon selkeimmät hyödyt liittyvät erityisesti valvomokokonaisuuden keskitettyyn hallintaan ja yhtenäiseen operatiiviseen tilannekuvaan kuntien tietoturvapoikkeamista. Keskitetyssä valvomoratkaisussa käytetyt toimintamallit, kuten poikkeamien luokittelu ja käsittely sekä valvonnassa käytetty teknologia olisi yhdenmukaista jokaiselle valvomoa käyttävälle kunnalle, joka lisää ratkaisun selkeyttä kuntien näkökulmasta.

Keskitetyllä tietoturvavalvomolla olisi myös mahdollisuus kohdistaa joustavasti resursseja sellaisiin kuntiin tai valvottaviin kohteisiin, missä niitä kulloinkin tarvitaan. Tämä voi kuitenkin aiheuttaa merkittävän riskin sellaisessa tapauksessa, jossa resursseja tarvitaan hetkellisesti enemmän kuin niitä on käytettävissä.

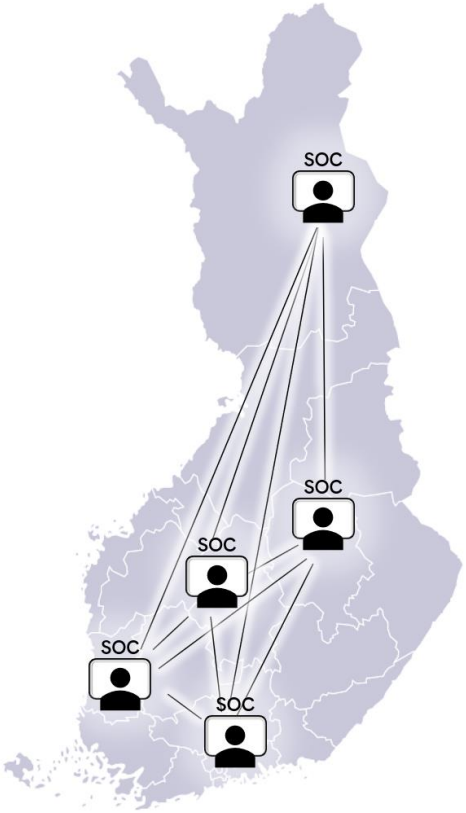
Keskitetyn tietoturvavalvomon olennaisimmat haasteet liittyvät kuntien vaihtelevaan tietoturvan kypsyystasoon sekä vaihtelevaan tapaan järjestää tietohallinnon toiminnot, kuten palvelut, tietoliikenneinfrastruktuuri ja tietojärjestelmät. Esimerkiksi tietoturvapoikkeamien käsittelyssä tarvittavien operatiivisten toimenpiteiden toteuttaminen olisi haasteellista tilanteessa, jossa tosiasiallista ylläpito- tai hallintaoikeutta kuntien tietojärjestelmiin ei olisi järjestettävissä. Jos tietoturvavalvomon riittävät hallintaoikeudet kuntien tietojärjestelmiin voitaisiinkin toteuttaa erityisjärjestelyin, vaatisi se siitä huolimatta valtavan määrän osaamista kunkin kunnan tietojenkäsittely-ympäristöistä ja niihin liittyvistä toimintamalleista.

Lisäksi uuden tietoturvavalvomon organisointi vaatisi erityisesti alkuvaiheessa merkittävän määrän käyttöönottoon ja perustamiseen liittyvää työtä tietoturvan valvontaan erikoistuneilta asiantuntijoilta, mikä aiheuttaa hyvin todennäköisesti pitkäaikaisia haasteita myös tarvittavan työvoiman saatavuudelle.

Keskitetyn tietoturvavalvomon tulisi kyetä tarjoamaan havainnointi- ja reagointipalvelut kaikille sen piirissä oleville kunnille riippumatta siitä, miten kunnat ovat tietohallintotoimintonsa järjestäneet. Mikäli kuntien tietohallintoon liittyvä palvelutuotanto olisi lähtökohtaisesti keskitetympää, olisi myös keskitetyn tietoturvavalvomon toteuttaminen yksinkertaisempaa ja siten myös helpommin perusteltavissa.

5.2 Alueelliset tai kuntakohtaiset tietoturvavalvomot

Alueellisten tai kuntakohtaisten tietoturvavalvomoiden järjestämisvaihtoehdon osalta kunnat päättäisivät nykyisen toimintamallin mukaisesti itse, miten ja miltä toimijalta sekä millaisin ominaisuuksin tietoturvavalvomopalvelu hankitaan.



Kuva 8. Alueelliset tai kuntakohtaiset tietoturvavalvomot

Yksi selkeimpiä alueellisten tai kuntakohtaisten tietoturvavalvomoiden toimintamallin etuja on kuntien mahdollisuus hyödyntää samoja rakenteita ja palveluverkostoja kuin muunkin tietohallinnon palvelutuotannon järjestämisessä. Tällöin tietoturvan valvonta tapahtuisi mahdollisimman lähellä järjestelmien ja palveluiden operatiivista tuottamista mahdollistaen siten suoraviivaisen ja nopean reagoinnin tietoturvapoikkeamiin.

Kuntakohtaisesti toteutettujen tietoturvavalvomoiden hankinta tai perustaminen vaatii kuitenkin kunnilta hankintaosaamista ja ymmärrystä tietoturvavalvomolle asetettavista teknisistä ja operatiivisista vaatimuksista. Kunnille toteutetuista haastatteluista ja kyselystä käy ilmi, että erityisesti asukasluvultaan pienehköillä kunnilla ei ole mahdollisuutta henkilöresurssien, hankintaosaamisen ja budjettinsa puitteissa perustaa tai ulkoistaa tietoturvavalvomoa itsenäisesti. Pienemmät kunnat hyötyisivätkin järjestelystä, jossa seudulliset keskuskunnat tai hyvinvointialueet, joilta löytyy sekä kokemusta tietoturvavalvomoiden hyödyntämisestä että tarvittavaa tietoturvaosaamista,

voisivat tukea erityisesti alueensa asukasluvultaan pienempiä kuntia kriittisimpien digitaalisten palveluiden ja tietojärjestelmien valvonnassa.

Paremman operatiivisen tilannekuvan koostamiseksi tietoturvavalvomoiden keskinäistä tiedonvaihtoa sekä viranomaisten suuntaan tapahtuvaa viestintää voitaisiin parantaa kehittämällä edelleen toimijoiden välisiä tiedonvaihtomalleja ja kanavia, jolloin tietoturvavalvomot muodostaisivat koko kuntatoimialan näkökulmasta hajautetun ja markkinaehtoisen verkoston.

5.3 Tiedonvaihto tietoturvavalvomoiden välillä

Tiedonvaihdon ja raportoinnin keskeisiä tarpeita kuntaorganisaatiolle ovat tietoturvan valvontaan liittyvien ajantasaisten uhka- ja indikaattoritietojen vaihto sekä tietoturva- ja tietosuojapoikkeamiin liittyvä raportointi tarvittaville viranomaistahoille. Ilman keskitettyä palvelutuotantoa ja tietoturvavalvomoa tiedonvaihdon tehokas järjestäminen vaatii tietoturvavalvomoiden, kuntien ja viranomaisten aktiivista osallistumista tiedonvaihtoon. Näiden toimijoiden keskinäistä tiedonvaihtoa kehittämällä voidaan saavuttaa vastaavia hyötyjä kuin keskitetyllä tietoturvavalvomolla, kuitenkin ilman keskitetyn tietoturvavalvomon asettamia haasteita.

Uhka- ja poikkeamatietojen vaihto

Tietoturvavalvomon näkökulmasta tehokas uhkien havainnointi ja torjunta edellyttää ajantasaista tietoa aktiivisista uhista ja hyökkäysmenetelmistä. Ajantasaisen tiedon saamiseksi voidaan hyödyntää muun muassa luotettaviksi tunnistettuja tietolähteitä sekä verkostoja tiedon jakamiseksi ja vaihtamiseksi.

Potentiaalisia tietolähteitä ovat muun muassa toimialaan liittyvät muut toimijat, kuten muiden kuntien tietoturvavalvomot, kunnille tietoteknisiä palveluita tuottavat organisaatiot, hyvinvointialueiden tietoturvavalvomot, kansallista tilannekuvaa ylläpitävät viranomaistahot sekä kansainväliset lähteet, kuten Euroopan Unionin viranomaiset ja muut jäsenvaltiot. Uhka- ja tilannetiedon kansalliseen tiedonvaihtoon käytettyjä ratkaisuja ovat erilaiset tilannekuvatuotteet ja tiedonvaihtoverkostot kuten esimerkiksi ISAC-tiedonvaihtoryhmät[12].

5.4 Tietoturvallisuuden ja tietoturvan valvonnan sisällyttäminen hankittaviin palveluihin

Yksi tapa parantaa kuntien digitaalista turvallisuutta on sisällyttää tietoturvan valvonta hankittaviin palveluihin muiden tietoturvallisuusvaatimusten ohella, jolloin palveluntarjoaja vastaa siitä, että toimitetun palvelun tai järjestelmän tietoturvan toteutumista valvotaan ja siitä raportoidaan säännöllisesti palvelun tilaajalle. Käytännössä tämä tarkoittaa sitä, että palvelun toimittamisesta ja tuotannosta laadittaviin sopimuksiin sisällytetään vaatimukset tietoturvan valvonnasta.

Tiedonhallintalautakunnan julkaiseman suositus tietoturvallisuudesta hankinnoissa[13] ja sen liitteenä oleva hankintaehtotyökalu[14] opastaa viranomaisia ja erityisesti hankintayksiköitä tietojärjestelmien ja soveltuvin osin muiden palveluiden hankintoihin

[12] ISAC-tiedonvaihtoryhmät, Liikenne- ja viestintävirasto Traficom 2023
[13] Suositus tietoturvallisuudesta hankinnoissa, Valtiovarainministeriön julkaisuja 2023:57
[14] Liite 2 a Hankintaehtotyökalu (uudet Excel-versiot), Valtiovarainministeriön julkaisuja 2023:57

liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön Julkriin[15] perustuva Hankintaehtotyökalu sisältää muiden vaatimusten ohella myös lukuisia tietoturvan valvontaan liittyviä merkittäviä vaatimuksia.

6 Suosituksia toimenpiteistä

Tässä selvityksessä käsiteltyjä vaihtoehtoisia ratkaisutapoja kuntien tietoturvavalvomoiden järjestämiseksi ovat keskitetty tietoturvavalvomo ja alueellisesti tai kuntakohtaisesti hajautetut tietoturvavalvomot. Ottaen huomioon kuntien tietohallinnon ja palvelutuotannon järjestämismallien monipuolisuuden sekä sen, että osa kunnista on jo kehittänyt omaa tai alueensa tietoturvan valvontaa, suositeltavin järjestämismalli on alueellisesti tai kuntakohtaisesti toteutettujen tietoturvavalvomoiden tukeminen ja jatkokehittäminen.

Toimenpiteitä tietoturvavalvomoiden toimintaedellytysten ja kuntien tietoturvan valvonnan kehittämiseksi ovat muun muassa:

- Informaatio-ohjauksen ja suositusten lisääminen,
- kuntien hankintojen ja kilpailutusten tukeminen,
- käyttöönoton kannustimet sekä
- tietojenvaihdon ja koordinaation kehittäminen.

Edellä mainittuja toimenpiteitä voidaan toteuttaa toisistaan riippumatta niiden kuitenkin tukiessa toinen toistaan vaiheittain.

Esimerkiksi informaatio-ohjaus sellaisenaan edesauttaa tietoturvavalvomoiden käyttöönottoon liittyvien päätösten tekemistä kunnissa, mutta tuettuna vaiheittaisilla hankintajärjestelyjen etukäteisvalmisteluilla ja käyttöönottoihin sekä kehittämiseen liittyvillä kannustimilla voidaan edelleen tukea tietoturvavalvomoiden laajempaa käyttöä kuntatoimialalla. Toimijoiden aktiivinen osallistuminen tietojenvaihtoon sekä tietojenvaihdon koordinaation edelleen kehittäminen edesauttaa erityisesti laajemman toimialakohtaisen kansallisen tilannekuvan muodostamista.

[15] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö, Valtiovarainministeriön julkaisuja 2022:43

7 Lähdeluettelo

1. **Valtiovarainministeriö.** Julkisen hallinnon digitaalinen turvallisuus, Valtiovarainministeriön julkaisuja 2020:23. [Online] 2020. https://julkaisut.valtioneuvosto.fi/handle/10024/162169

2. **Valtiovarainministeriö.** Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka), Valtiovarainministeriön julkaisuja 2020:33 [Online] 2020. https://julkaisut.valtioneuvosto.fi/handle/10024/162191

3. **Digi- ja väestötietovirasto**. Digitaalisen turvallisuuden arkkitehtuuri. [Online] 2022. https://wiki.dvv.fi/display/DTARK/

4. **Laki julkisen hallinnon tiedonhallinnasta**. 906/9.8.2019. [Online] 2019. https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

5. **Valtiovarainministeriö.** Tiedonhallintalautakunta. [Online] 2023. https://vm.fi/tiedonhallintalautakunta

6. **Euroopan parlamentti ja neuvosto.** Direktiivi (EU) 2022/2555, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi). [Online] 2022. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022L2555&qid=1693498383839

7. **Valtioneuvosto.** Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä, LVM044:00/2022. [Online] 2022. https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022

8. **Euroopan parlamentti ja neuvosto.** Asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). [Online] 2016. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679

9. **Euroopan parlamentti ja neuvosto.** Ehdotus asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten. [Online] 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

10. **Digi- ja väestötietovirasto.** Digitaalisen turvallisuuden arkkitehtuuri: Nollaluottamusmallin periaatteet. [Online] 2022. https://wiki.dvv.fi/display/DTARK/Nollaluottamusmallin+periaatteet

11. **Kuntaliitto.** Kuntien tietohallinnon roolit. [Online] 2022. https://www.kuntaliitto.fi/julkaisut/2022/2216-kuntien-tietohallinnon-roolit

12. **Liikenne- ja viestintävirasto Traficom.** ISAC-tiedonvaihtoryhmät. [Online] 2023. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

13. **Tiedonhallintalautakunta.** Suositus tietoturvallisuudesta hankinnoissa, Valtiovarainministeriön julkaisuja 2023:57. [Online] 2023. https://julkaisut.valtioneuvosto.fi/handle/10024/165075

14. **Tiedonhallintalautakunta.** Suositus tietoturvallisuudesta hankinnoissa Liite 2 a Hankintaehtotyökalu (uudet Excel-versiot), Valtiovarainministeriön julkaisuja 2023:57. [Online] 2023. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165075/Liite%202%20a%20Hankintaehtoty%c3%b6kalu%20%28uudet%20Excel-versiot%291.01.xlsx?sequence=8&isAllowed=y

15. **Tiedonhallintalautakunta.** Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö, Valtiovarainministeriön julkaisuja 2022:43. [Online] 2022. https://julkaisut.valtioneuvosto.fi/handle/10024/164183

Liite 1 Tietoturvauhkien nykytila ja Euroopan Unionin kyberturvallisuusviraston näkemys ajankohtaisista uhkista

Tietoturvauhkien kytkeytyminen digitalisaation nopeaan etenemiseen

Digitalisaation ensimmäisinä vuosikymmeninä tietoturvan riskitaso oli globaalisti varsin matala. Ajan saatossa tietoturvan uhkamaasto on muuttunut dramaattisesti, sillä jatkuvasti etenevä ja laajentuva digitalisaatio on merkinnyt tietojärjestelmiin ja tietovarantoihin talletetun tiedon rikastumista, sen rahallisen arvon nousua ja siitä saatavan rikoshyödyn kasvua.

Rikollisilla on digitalisaation myötä käytössään uusi globaali ulottuvuus, joka ei tunne valtiollisia rajoja sekä lähes taattu anonymiteetti. Lisäksi rikoksiin tarvittavat välineet saa hankittua helposti ja kohtuullisen pienin investoinnein. Alalle tulon kynnys on matala, rikosten taloudellinen potentiaali valtava, ja kiinnijäämisen riskit usein pieniä. Digitaaliseen toimintaympäristöön kohdistuvan rikollisuuden määrä on kasvanut nopeasti ja se on myös organisoidulle rikollisuudelle hyöty-riskisuhteeltaan houkuttelevampi kuin useat muut rikollisuuden lajit.

Euroopan Unionin kyberturvallisuusviraston ENISA:n näkemys ajankohtaisista kyberturvallisuusuhkista

Euroopan Unionin kyberturvallisuusvirasto ENISA (*The European Union Agency for Cybersecurity*) julkaisee säännöllistä raporttia tietoturva- ja kyberturvallisuusuhkien kokonaistilasta ja viimeaikaisista muutoksista. Vuoden 2022 lopussa julkaistu raportti nostaa nykytilanteesta esille ennen kaikkea:

- Geopoliittisen tilanteen muutokset Venäjän Ukrainaa vastaan aloittaman hyökkäyssodan vaikutuksesta. Sotilasoperaatioihin on konfliktissa liitetty laajamittaisesti kyberhyökkäyksiä, joiden tarkoitus on ollut lamauttaa kohteena olleiden tietojärjestelmien toimintakyky. Kohteena eivät ole olleet pelkästään sotilasjärjestelmät, vaan myös maan hallintoon, lentoliikenteeseen ja energiasektoriin liittyvät tietojärjestelmät.

- Teknisesti entistä kehittyneemmät hyökkäykset, esimerkiksi:

    - Julkaisemattomien haavoittuvuuksien eli niin kutsuttujen *nollapäivähaavoittuvuuksien* entistä yleisempi käyttö. Ohjelmistoissa, käyttöjärjestelmissä ja jopa itse prosessoreissa rautatasolla olevia julkaisemattomia haavoittuvuuksia vastaan on vaikeaa, ellei jopa mahdotonta rakentaa pitäviä suojauksia.

    - Kaupallisten tietomurtopalvelujen lisääntyminen, mikä mahdollistaa hyökkääjälle teknisen hyökkäyskyvykkyyden nostamisen ammattimaiselle tasolle omasta kyvykkyydestä riippumatta.

    - Kolmansien osapuolien kautta tehdyt laajamittaiset toimitusketjuhyökkäykset. Näissä hyökkäyksissä murretaan ensin kohteena olevien organisaatioiden käyttämien ulkopuolisten ohjelmistotuotteiden tai palveluiden tietoturva. Tämän jälkeen murrettujen tuotteiden tai palveluiden

kautta hyökätään niitä käyttäviä organisaatioita vastaan. Taktiikkaa käytetään erityisesti sellaisia kohteita vastaan, joiden omat suojaustoimenpiteet ovat vahvoja. Menetelmää voidaan käyttää myös laajamittaiseen organisaatiojoukkoon vaikuttamiseen kerralla silloin, kun murrettu ohjelmisto tai palvelu on hyvin yleisesti käytössä eri organisaatioissa.

- Kiristyshaittaohjelmien yleistyminen edelleen
- Lisääntyneet hyökkäykset tietojen ja palveluiden saatavuutta vastaan
- Uusien uhkien ja hybridiuhkien ilmaantuminen, esimerkiksi:
    - päästä-päähän salattujen yhteyksien salakuuntelu asentamalla päätelaitteisiin vakoiluohjelma. Salakuunteluun käytettävien, edistyneiden vakoiluohjelmien asennus voidaan usein tehdä verkon yli ilman, että käyttäjän on mahdollista havaita asiaa,
    - kalasteluhyökkäysten uskottavuuden kehittäminen tasolle, jolla niitä on vaikea erottaa oikeista, kohteen mahdollisesti käyttämien palveluntarjoajien yhteydenotoista,
    - koneoppimisen ja tekoälyn etujen hyödyntäminen rikollisissa tarkoituksissa, sekä
    - koneoppimiseen ja tekoälyn käyttöön liittyvien uudentyyppisten tietoturvahaavoittuvuuksien etsiminen ja hyödyntäminen.

Yhteenveto

Digitalisaation alkuvaiheessa vallinneessa, suhteellisen matalan ristitason ilmapiirissä tietoturvaa rakennettiin pitkälti suojauksen näkökulmasta, rakentamalla esteitä mahdollisten hyökkäysten varalta. Viime aikojen uhkatrendien mukaisesti hyökkääjän todennäköisyys murtaa kohteen suojausmekanismit on kuitenkin merkittävästi kasvanut. Sen jälkeen ainoastaan järjestelmien tehokas valvonta voi estää tunkeutujien pitkäaikaisen asettumisen haltuun otettuihin järjestelmiin.

Digitaalisessa turvallisuudessa, samoin kuin fyysisessä turvallisuudessa, estävät toimenpiteet muodostavat vain osan ympäristön turvallisuudesta, muiden yhtä merkittävien rakennusosien ollessa ympäristön tehokas valvonta, oikeudettomien tahojen poistaminen suojattavasta ympäristöstä ja kyvykkyys ympäristön turvallisuuden tehokkaaseen palauttamiseen.

Liite 2: Kansainvälinen katsaus julkisen hallinnon tietoturvavalvomotoimintoihin

Kansainvälisessä katsauksessa tarkastellaan sekä kyberturvallisuuteen liittyvää Euroopan Unionin lainsäädäntöä ja aloitteita että yksittäisiä maita. Yksittäisistä maista katsaukseen valittiin Yhdysvallat ja Iso-Britannia, sillä nämä maat esitetään usein kansalliseen kyberpuolustukseen ja -turvallisuuteen liittyvissä lähteissä kyberpuolustuksen kärkimaina.

Euroopan unioni

Euroopan unionin kyberturvallisuuteen liittyvistä aloitteista keskeisiä ovat Euroopan komission tiedonannot Euroopan unionin kyberturvallisuusstrategiasta (JOIN(2020) 18), kyberpuolustuspolitiikasta (JOIN(2022) 49) ja komission ehdotus asetuksesta kybersolidaarisuudesta ja kyberkilvestä (engl. *Cyber Solidarity Act ja European Cyber Shield*) (COM(2023) 209). Yhdessä ne muodostavat eheän jatkumon Euroopan Unionin ja sen jäsenvaltioiden kybertuvallisuuden tavoitellulle kehitykselle alkuperäisestä strategiamietinnöstä lainsäädännölliseen asetusehdotukseen. Selvityksen kirjoitushetkellä komission ehdotuksen lainsäädäntöprosessi on vielä kesken.

Ehdotuksen taustoituksessa todetaan, että tieto- ja viestintätekniikoiden käytöstä on tullut perustekijöitä kaikilla taloudellisen toiminnan sektoreilla, kun julkishallinto, yritykset ja kansalaiset ovat entistä enemmän riippuvaisia toisistaan yli sektoreiden ja maiden rajojen. Samaan aikaan kyberturvallisuuspoikkeamat ovat entistä laajempia, yleisempiä ja vaikutuksiltaan voimakkaampia. Nykyisen uhkamaaston luonteeseen kuuluvat myös geopoliittiset jännitteet ja digitaalisen toimintaympäristön hyödyntäminen poliittisiin ja ideologisiin tarkoituksiin.

Tämän vuoksi Euroopan Unioni ehdottaa jäsenvaltioidensa kyberturvallisuusuhkien ja -poikkeamien havaitsemiskyvyn parantamista, jäsenvaltioiden keskinäisen yhteistyön ja kybersolidaarisuuden lisäämistä sekä reagointivalmiuden nostamista merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien varalta.

Uhkien ja poikkeamien havainnointikyvyn parantamiseksi ehdotetaan otettavaksi käyttöön Euroopan Unionin kattava tiedonjako- ja tietoturvavalvomoinfrastruktuuri (ns. ”kyberturvallisuuden eurooppalainen suojakilpi”), jonka käytännön toteutus olisi koko Euroopan Unionin laajuinen verkosto yli rajojen toimivia kyberturvallisuuden operaatiokeskuksia (*cross-border SOCs*). Nämä keskenään verkottuneet operaatiokeskukset puolestaan kytkeytyisivät jäsenvaltioiden kansallisiin keskuksiin, ja suojakilven toteuttamiseksi ehdotetaan kansallisen operaatiokeskuksen perustamista kussakin jäsenmaassa pakolliseksi.

Ehdotuksessa kybersolidaarisuus ulottuu uhka-, havainto- ja poikkeamatietojen jakamisen lisäksi vakavien kyberhyökkäysten kohdalla avunantoon yli jäsenmaiden rajojen. Avunantoa varten ehdotetaan perustettavaksi Euroopan Unionin tasolla kyberturvallisuusreservi, joka koostuisi yksityisten tietoturvapalveluntarjoajien palveluista.

Ehdotukseen kuuluu myös aie varustaa suojakilpeen osallistuvat toimijat uusimman tekniikan tason mukaisilla välineillä, laitteilla ja infrastruktuurilla sekä tehostaa suojakilven toimintaa erityisesti viimeisimpien tekoäly- ja data-analytiikkateknologioiden avulla.

Taloudellisesti asetuksen täytäntöönpanoa tuettaisiin Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskevan strategisen tavoitteen mukaisella rahoituksella. Kokonaistalousarvio sisältää 100 miljoonan euron lisäyksen, jota ehdotetaan tässä asetuksessa kohdennettavaksi uudelleen Digitaalinen Eurooppa -ohjelman (*The Digital Europe Programme*) muista strategisista tavoitteista. Tämä nostaa Digitaalinen Eurooppa -ohjelman mukaisia kyberturvallisuustoimia varten käytettävissä olevan uuden kokonaissumman 842,8 miljoonaan euroon.

Yhdysvallat

Yhdysvaltojen kyberturvallisuuskehitys seuraa varsin samantyyppistä linjaa Euroopan Unionin kyberturvallisuuskehityksen kanssa. Maaliskuussa 2023 julkaistun kansallisen kyberturvallisuusstrategian *(National Cybersecurity Strategy)* myötä Yhdysvallat asettaa kyberturvallisuuden tärkeäksi osaksi kansallista turvallisuusstrategiaansa vastatakseen kasvaviin kyberuhkiin sekä valtiollisten että muiden toimijoiden suunnalta. Valtiollisista toimijoista kyberturvallisuusstrategiassa nimetään Venäjä, Kiina, Iran ja Pohjois-Korea.

Lainsäädännöllisesti Yhdysvallat on ottanut kyberturvallisuuteen liittyen käyttöön työkaluja, mukaan lukien *Cybersecurity Information Sharing Act*in, vahvistaakseen tiedonvaihtoa liittovaltion hallinnon ja yksityisen sektorin välillä, pitkälti samoista syistä kuin muissakin länsimaissa. Myös Yhdysvalloissa sotilaallisesti ja kansallisesti merkittävät järjestelmät ovat osin myös yksityisen sektorin hallinnassa. Etenkin tämä koskee Yhdysvalloissa kriittisen infrastruktuurin järjestelmiä.

Keskeisessä roolissa kyberturvallisuuden alueella toimii liittovaltion virastoista *Department of Homeland Security (DHS)* ja sen alla *Cybersecurity and Infrastructure Security Agency (CISA)*, jolla on operatiivinen johto kriittisen infrastruktuurin suojelemisessa ja sen kyberresilienssin rakentamisessa. Myös *National Security Agency (NSA)* on edelleen merkittävässä asemassa, erityisesti signaalitiedustelun ja kyberoperaatioiden alueilla.

Tietoturvavalvomoiden käyttöönotto nähdään oleellisena osana kyberpuolustusstrategiaa, ja valtiollisesti *Department Of Justice (DOJ)* tarjoaa liittovaltion hallinnon organisaatioille jatkuvaa ympärivuorokautista tietoturvavalvomopalvelua kattavalla palveluvalikoimalla *(Security Operations Center as a Service, SOCaaS)*:

- Ajantasainen tilannekuva uhkamaastosta
- Verkkojen ja järjestelmien valvonta
- Uhkien aktiivinen metsästys valvottavassa infrastruktuurissa siihen erikoistuneiden tietoturva-asiantuntijoiden voimin (*threat hunting*)
- Tunkeutumisten havaitseminen ja poistaminen
- Tunkeutumisten jälkeinen forensiikka

- Asiakasportaali asiakaskohtaisten avaintietojen ja -mittareiden seurantaan

Palvelu sisältää myös asiakaskohtaisen räätälöinnin ja jatkuvan tuen.

Yhdysvalloissa on lisäksi käynnistetty aloitteita kyberturvallisuuteen liittyvän osaamisen lisäämiseksi ja vahvistamiseksi, kuten *National Initiative for Cybersecurity Education (NICE)*.

Iso-Britannia

Myös Iso-Britannia on nostanut korkealle kyberturvallisuuden merkityksen valtiollisessa kehyksessä. Kyberturvallisuusstrategiassa vuosille 2022–2030 pyritään ensi vaiheessa nostamaan vastustuskykyä kyberhyökkäyksiä vastaan merkittävästi vuoteen 2025 mennessä, ja kaikkien hallituksen keskeisten, virallisten tietojärjestelmien tavoitellaan olevan suojattuna tunnetuilta haavoittuvuuksilta vuoteen 2030 mennessä. Erityinen paino strategiassa asetetaan hyvien tietoturvakäytäntöjen käyttöönottoon.

Strategia nojaa kahteen strategiseen peruspilariin: organisaatioiden kyberturvallisuuden vahvistamiseen riskienhallinnan kautta sekä solidaariseen yhteispuolustukseen. Havaintoverkko muodostuu solidaarisen yhteispuolustuksen periaatteen kautta luontaisesti hajautetuksi, nojaten vahvasti organisaatioiden väliseen yhteistiedonkeruuseen ja laajamittaiseen, automaattiseen havaintotiedon jakeluun.

Tärkeisiin aloitteisiin kuuluu NSCS (*National Cyber Security Centre*) kehittämän CAF (*Cyber Assurance Framework*) -kyberarviointikehyksen käyttöönotto, hallituksen kyberkoordinointikeskuksen perustaminen tietojen jakamisen tehostamiseksi, 'secure by design' -filosofian järjestelmällinen käyttöönotto sekä yhteisten kyvykkyyksien, kuten aktiivisen kyberpuolustuksen kehittäminen. Kybervasteessa osalta keskitytään nostamaan reagointikyvykkyyttä sekä valmistautumisen että käytännön harjoitusten kautta. Kuten Euroopan Unionin ja Yhdysvaltojenkin strategioissa, tekoälyn käytön lisäämistä puolustuksessa suunnitellaan ja kyberosaamiseen panostamisen tärkeys tunnistetaan keskeisenä tekijänä.

Lähteet

1. **ITU**: Global Cybersecurity Index. [Online] 2023. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
2. **Analytics Insights**: Top 6 Countries with the Best Cyber Security Measures. [Online] 2019. https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/
3. **Euroopan parlamentti ja neuvosto**. Tiedonanto: EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle. [Online] 2020. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52020JC0018
4. **Euroopan parlamentti ja neuvosto**. Tiedonanto: EU:n kyberpuolustuspolitiikka. [Online] 2022. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52022JC0049
5. **Euroopan parlamentti ja neuvosto**. Asetusluonnos toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten. [Online] 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209
6. **Valkoinen talo (Yhdysvallat)**. National Cybersecurity Strategy 2023 (USA). [Online] 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
7. **Department of Justice (Yhdysvallat).** Security Operations Center as a Service SOCcaaS (DOJ) (USA). [Online] 2023. https://www.cisa.gov/resources-tools/services/security-operations-center-service-socaas
8. **Ison Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan keskushallitus (UK)**. Government Cyber Security Strategy: 2022 to 2030. [Online] 2022. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030