Helsingin kaupungin tietomurto 2024

P2024-01

ALKUSANAT

Valtioneuvosto päätti 4.7.2024 aloittaa Helsingin kaupunkiin kohdistuneen tietomurron tutkinnan ja asetti Onnettomuustutkintakeskuksen yhteyteen itsenäisen ja riippumattoman tutkintaryhmän. Tutkintapäätös perustuu turvallisuustutkintalain (525/2011) 32 §:ään. Kyseessä on turvallisuustutkintalain 5. luvun mukainen poikkeuksellisen tapahtuman tutkinta.

Tutkintaryhmän johtajaksi nimettiin johtava tutkija, dosentti Hanna Tiirinki ja jäseniksi KTT, PsM Petri Koistinen, HTM Ville-Petteri Pulkkinen, datanomi Kimmo Rousku, DI Petteri Järvinen, DI Tomi Lounema ja BBA, MA Lilly Korpiola.

Lainsäädännön erityisasiantuntijaksi nimettiin viestintäoikeuden professori, varatuomari Päivi Korpisaari.

Tapausta tutkii myös Keskusrikospoliisi.

Poikkeuksellisen tapahtuman tutkinta toteutetaan turvallisuustutkinnan periaatteilla. Turvallisuustutkinnan tarkoituksena on yleisen turvallisuuden lisääminen, eikä tutkintaa tehdä oikeudellisen vastuun kohdentamiseksi.

Turvallisuustutkinnassa selvitetään tapahtumien kulku, syyt ja seuraukset sekä tehdyt pelastustoimet ja viranomaisten toiminta.

Tutkintaselostus sisältää selostuksen tapahtumien kulusta, niihin johtaneista tekijöistä ja seurauksista sekä asianomaisille viranomaisille ja muille toimijoille osoitetut turvallisuussuositukset sellaisiksi toimenpiteiksi, jotka ovat tarpeen yleisen turvallisuuden lisäämiseksi, vahinkojen torjumiseksi sekä pelastus- ja muiden viranomaisten toiminnan tehostamiseksi.

Tutkintaselostus on ollut lausunnolla keskeisimmällä tapahtumaan osallisilla toimijoilla. Lausunnot on otettu huomioon tutkintaselostusta viimeistellessä. Yhteenveto lausunnoista on tutkintaselostuksen lopussa.

Tutkintaselostuksessa käytetyt graafit ja kuvituksen tutkintaryhmälle on tehnyt Sole Lätti/ Tiedekuvitus. Näiden graafien kuvien lähdettä ei ole erikseen merkitty selostukseen.

Tutkintaselostuksen on kääntänyt ruotsin ja englannin kielelle Lingsoft.

Tutkintaselostus annettiin valtioneuvostolle 17.6.2025 ja se julkaistiin Onnettomuustutkintakeskuksen verkkosivuilla osoitteessa *www.turvallisuustutkinta.fi*.

Tutkinnan tunnus: P2024-01
Tutkintaselostus 3/2025
ISBN: 978–951–836–677–8 (PDF)
ISSN: 2341–5991

SISÄLLYSLUETTELO

1 TAPAHTUMAT

Helsingin kaupungilla havaittiin laaja tietomurto 30.4.2024. Tietomurto kohdistui Kasvatuksen ja koulutuksen toimialan (KASKO) verkkoon ja sen palvelimiin. Asian tultua ilmi kaupunki käynnisti vastatoimet ja onnistui pysäyttämään hyökkäyksen. Tietomurron todellista laajuutta ei alkutilanteessa kyetty hahmottamaan, sillä tietomurron kohteiden selvitystyö vei aikaa.

Tietomurron vaiheet ja hallintatoimet kuvataan seuraavissa kappaleissa. Tiedot on kerätty analysoimalla tapahtuman jälkeen erilaisia lokeja,[1] mutta koska kaikkia tarvittavia lokitietoja ei ollut saatavilla, aukotonta kuvaa tapahtumista ei ole pystytty muodostamaan.

1.1 Tietomurron vaiheet

Keväällä 2024 tuntematon hyökkääjä yritti tunkeutua KASKOn verkkoon etsimällä verkosta heikkouksia ja kokeilemalla eri salasanoja. Aikavälillä 29.2.-4.4.2024 rekisteröitiin yli 300 000 yhteydenottoa. Yritykset kohdistuivat ulospäin näkyvään VPN-reitittimeen,[2] joka kuitenkin torjui yritykset.

Toinen, eri osoitteesta tullut hyökkääjä keräsi tietoa KASKOn verkkoympäristöstä 15.3.2024 ja kokeili salasanoja 8.-12.4.2024 välisenä aikana. Hyökkääjä yritti murtautua VPN-reitittimelle käyttäen kahta tunnettua haavoittuvuutta. Yritykset johtivat teknisesti vanhentuneen ja ilman päivityksiä jääneen reitittimen kaatumiseen 14.4.2024 klo 20:14, mutta eivät avanneet pääsyä sisäverkkoon. Ne tuottivat kuitenkin lisää tietoa VPN-laitteesta ja verkkotekniikasta, jota hyökkääjä pystyi myöhemmin hyödyntämään. Puutteellisen valvonnan vuoksi murron valmistelua ei havaittu KASKOn omassa seurannassa.

Jälkimmäinen hyökkääjä onnistui kirjautumaan VPN-reitittimelle mahdollisesti jo 18.4.2024, mutta varsinainen tietomurto käynnistyi 25.4.2024 klo 13:17, kun hyökkääjä kirjautui KASKOn sisäverkkoon hyödyntämällä pimeästä verkosta[3] löytämäänsä yläkoulun oppilaan käyttäjätunnusta ja salasanaa.

Onnistuneen murron jälkeen hyökkääjä kartoitti sisäverkkoa skannaamalla kahden tunnin aikana 34 verkkoporttia yhteensä 9 945:ssa sisäverkon IP-osoitteessa. Toimet aiheuttivat palomuurilokeihin hälytyksiä 25.4.2024 klo 13:40 ja klo 13:59, mutta koska kaupungilla ei ollut käytössä palomuurin tietoturvahälytysten valvontapalvelua, ilmoituksiin eri reagoitu.

Hyökkääjä kirjautui klo 15:07 ensimmäisen kerran etätyöpöytäyhteydellä KASKOn palvelinympäristöön. Pian tämän jälkeen DigiHelsingin ylläpitämä haittaohjelmien torjuntaohjelmisto antoi vakavuudeltaan keskitason hälytyksen, jonka mukaan Windows-palvelimelta oli yritetty kirjautua yhdeksälle muulle palvelimelle yhteensä 122 kertaa.

---

[1] IT-ympäristössä lokitiedostoon kerätään järjestelmän, sovellusten tai verkon automaattisesti tuottamaa lokitietoa, joka tallentaa tapahtumia, käyttäjätoimintoja, järjestelmävirheitä ja tietoturvaan liittyviä tapahtumia analysointia, vianmääritystä ja valvontaa varten.

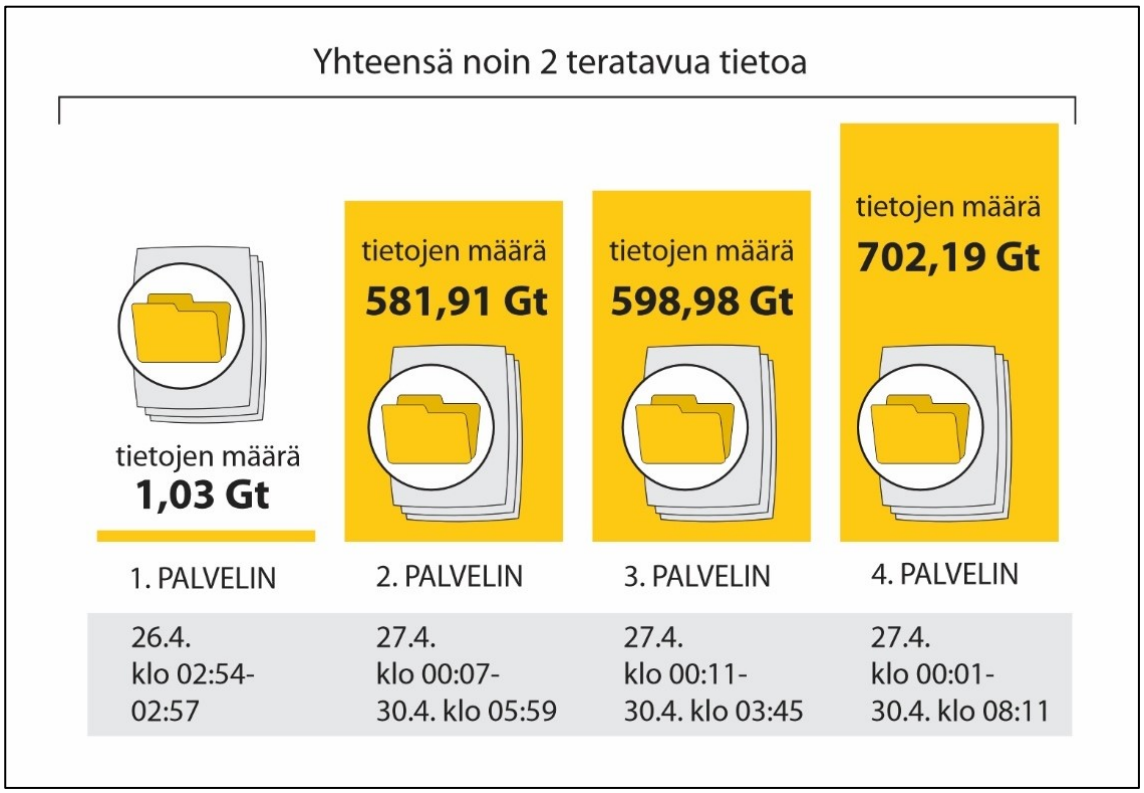
[2] VPN (Virtual Private Network) on tekniikka, jossa julkisen internet-verkon läpi luodaan suojattu tunneli. Sen avulla etäkäyttäjät voivat kytkeytyä turvallisesti sisäverkon palvelimille.

[3] Pimeä verkko on internetin alue, johon pääseminen vaatii erillisen TOR-selaimen. Siellä olevat verkkorikollisten kauppapaikat myyvät rikollisten tarvitsemia palveluita sekä käyttäjätunnuksia, salasanoja ja luottokorttitietoja.

DigiHelsingin palveluntarjoaja avasi havainnoista keskimääräisen vakavuustason tiketin[4] 25.4.2024 klo 17:22. Tiketti ohjautui klo 18:36 toiselle palveluntarjoajalle, mutta tiketöintijärjestelmässä olleen virheen vuoksi tiketti ei mennyt perille.

Hyökkääjä jatkoi kirjautumisia 25.4.2024 klo 16:36 alkaen etätyöpöytäyhteydellä KASKOn palvelinympäristöön ja sai 25.4.2024 klo 17:24 – 18:40 välisenä ajankohtana haltuunsa kahden eri toimialueen Active Directory -käyttäjähakemiston tiedot. Lisäksi hyökkääjä sai haltuunsa KASKOn keskeisen Windows-palvelimia sisältävän virtuaalipalvelinympäristön hallintapalvelimen.[5] Hyökkääjä onnistui myös murtautumaan KASKOn palvelinten ja tiedostojen varmuuskopioinnista vastaavaan palvelinympäristöön. Palvelinten haltuunoton ja tätä seuranneen tietojen kopioinnin mahdollisti tarvittavien toimialueiden pääkäyttäjien (administrator) salasanojen varastaminen.

Saatuaan tarvitsemansa tunnukset ja käyttöoikeudet palvelimiin hyökkääjä alkoi kopioida verkkolevyllä sijaitsevia KASKOn tiedostoja itselleen. Ensimmäinen tiedostosiirto alkoi 26.4.2024 klo 2:54, jolloin hyökkääjä kopioi KASKOn verkkolevyltä 1,03 gigatavua[6] tietoa. Testisiirron jälkeen hyökkääjä aloitti verkkolevyn tiedostojen varastamisen käyttäen apunaan kolmea sisäverkon palvelinta. Tiedostojen siirto-operaatio niiltä alkoi 27.4.2024 klo 0:01. Neljässä siirrossa kopioitiin yhteensä noin kaksi teratavua tietoa. Viimeisen palvelimen tiedostosiirto päättyi 30.4.2024 aamulla klo 8:11.



Kuva 1. Hyökkääjän tekemät tiedostosiirrot Helsingin kaupungin tietomurrossa.

[4] Tiketti on määrämuotoinen viesti, jolla ilmoitetaan havainnosta tai ongelmasta. Vastaanottaja ryhtyy toimenpiteisiin ja sulkee tiketin, kun asia on käsitelty loppuun.

[5] Virtuaalipalvelinympäristö koostuu erittäin suorituskykyisestä fyysisestä palvelinympäristöstä, jossa on paljon työ- ja levymuistia, ja jossa voi olla samanaikaisesti toiminnassa kymmeniä tai satoja virtuaalisia Windows- tai Linux-palvelinohjelmistoja.

[6] Gigatavu (Gt) on muistin määrän yksikkö (miljardi tavua). Muisti voi olla sisäistä työmuistia (RAM) tai pysyvää tallennustilaa (kiintolevyt, USB-tikut ym.). Teratavu on 1024 gigatavua.

Sisäverkon valvonnan ja palvelinten puutteellisen lokituksen vuoksi täydellistä listausta kopioiduista tiedostoista tai niiden määrästä ei pystytty selvittämään. Hyökkääjä kopioi tietoja ensisijaisesti Suomen aikaan yöllä, mikä pienensi kiinnijäämisen riskiä.

DigiHelsingin palvelutoimittaja havaitsi jonoon (on hold) jääneen tiketin vasta 29.4.2024 klo 11:34 tarkastuksessa, joita tuohon aikaan tehtiin säännöllisesti integraatio-ongelmien tunnistamiseksi. Samalla havaittiin, että tiketin tärkeysaste oli luokiteltu keskitasolle (medium), vaikka oikeampi taso olisi ollut kriittinen. Luokitus ei vaikuttanut tiketin perillemenoon, mutta kriittisen tason tiketin perillemeno oli sovittu varmistettavaksi puhelinsoitolla.

KASKOn IT-henkilöt saivat tiedon 25.4.2024 havaituista epäilyttävistä kirjautumisista ja salasanojen murtoyrityksistä vasta 29.4.2024 klo 11:54 lähetetyllä sähköpostilla. Asian selvittäminen KASKOssa aloitettiin, mutta sitä hidasti samaan aikaan tekeillä olleet palvelinten muutostyöt. Pidettiin mahdollisena, että varoitukset olivat palvelinten muutostöiden vuoksi aiheettomia.

Hyökkääjä yritti 29.4.2024 saada haltuunsa myös muita Windows-palvelimia murtamalla niiden salasanoja. Hyökkääjä käynnisti 30.4.2024 klo 01:30 väsytyshyökkäyksen[7] päästäkseen kahdelle muulle Helsingin kaupungin toimialueelle, jolloin kohteena oli yhteensä 165 verkossa olevaa laitetta. Samana yönä klo 03:10 hyökkääjä yritti keräämiensä tietojen avulla päästä myös muiden Helsingin kaupungin toimialueiden verkkoihin.

Yritykset tunkeutua KASKOn ympäristön ulkopuolelle kyselemällä hallintatunnuksia DigiHelsingin AD-palvelimelta tuottivat yöllä kriittisen tason hälytyksen, minkä seurauksena DigiHelsingin palvelutoimittaja lukitsi tunnukset. Tietomurto alkoi paljastua, kun DigiHelsingin työntekijä otti 30.4.2024 klo 8:55 Teamsilla yhteyttä KASKOn työntekijään asian selvittämiseksi.

1.2 Tietomurron havaitseminen ja toimenpiteet

Tiedot yöllä havaitusta tietomurrosta tuotiin 30.4.2024 klo 9:30 KASKOn pilvipalvelutiimin kokoukseen. Sen jälkeen selvitystyötä jatkettiin yhdessä DigiHelsingin kanssa. Kävi ilmi, että kyse oli vakavasta tapahtumasta, sillä murtautuja oli kopioinut itselleen verkkolevyllä olleita asiakirjoja. KASKOlla päätettiin kutsua koolle kaupunkitason vakavien häiriöiden MIM-ryhmän (Major Incident Management[8]) kokous samana päivänä klo 13:00, minkä jälkeen MIM-kokouksia järjestettiin säännöllisesti.

Aamupäivän kuluessa KASKOn ja DigiHelsingin asiantuntijat paikansivat hyökkääjän sisääntuloreitin VPN-laitteeseen. Sen yhteys kaupungin tietoverkkoon katkaistiin 30.4.2024 klo 13:40. Laitteen verkkokaapeli irrotettiin konesalissa sisäverkosta klo 14:30, mutta laitetta ei sammutettu, jotta sen muistissa olevat tiedot saataisiin säilytettyä.

Menetettyään yhteyden KASKOn verkkoon hyökkääjä jatkoi kirjautumisyrityksiä ainakin viikon ajan, mahdollisesti pidempäänkin. Yritykset eivät kuitenkaan onnistuneet, koska sisäänpääsyreitti oli tukittu katkaisemalla VPN-reitittimen yhteydet.

Kun tietomurron jälkiä tutkittiin, havaittiin 8.5.2024 klo 16:28 että myös toimialueen ulkopuolisella varmuuskopiointipalvelimella oli epätavallista toimintaa. Laite eristettiin verkosta, minkä jälkeen tarkistusohjelma löysi sen levyltä tietomurroissa usein käytetyn Neshta-haittaohjelman[9] eri versioita. Haittaohjelma oli vahingoittanut käyttöjärjestelmää niin,

[7] Väsytyshyökkäyksessä (engl. brute force) kokeillaan järjestelmällisesti erilaisia salasanavaihtoehtoja, kunnes oikea löytyy.
[8] MIM-ryhmä on organisaation tiimi, joka vastaa suurten ja kriittisten häiriötilanteiden hallinnasta.
[9] Neshta on vanha haittaohjelma, josta on useita versioita. Se kerää järjestelmästä ja käyttäjistä tietoja, jotka ovat hyödyksi tietomurron tekijälle.

ettei palvelin enää toiminut eivätkä varmuuskopiot olleet käyttökelpoisia. Toipuminen ja verkon puhdistaminen onnistuivat kuitenkin ilman varmuuskopioita.

KASKO käynnisti korjaustoimenpiteet uuden varmuuskopiointipalvelun toteuttamiseksi. Tietomurron aktiiviset tekniset hallintatoimet päätettiin ja KASKOn tietojärjestelmien katsottiin olevan näiltä osin turvallisessa tilassa.

Tutkintaryhmän käytössä olleet raportit osoittivat, että hyökkääjä oli yrittänyt murtautua yhteensä 1 700 Helsingin kaupungin verkossa olleeseen tietokoneeseen. Joukossa oli myös Helsingin yksityiskouluja, mutta yritykset epäonnistuivat.

1.3 Tietomurron hallintatoimien johtaminen

Helsingin kaupunki käynnisti järjestelmällisen tietomurron hallintatoimien johtamisen ensimmäisen MIM-ryhmän kokouksen myötä 30.4.2024 klo 13:00. Kaupunki ja KASKO asettivat tapahtuman johtamiseksi ja hallitsemiseksi seuraavia ryhmiä:

MIM-ryhmä häiriötilanteen hallintaan kokoontui ensimmäisen kerran 30.4.2024 klo 13:00 ja sen jälkeen toukokuun ajan päivittäin (yhteensä 32 kokousta). Kesäkuusta alkaen ryhmä kokoontui edelleen säännöllisesti useamman kerran viikossa.

Kasvatuksen ja koulutuksen toimialan kriisiryhmän (KASKO MIM-ryhmä) tehtävänä oli jakaa ja ylläpitää tilannekuvaa oman toimialansa osalta. Ryhmä kokoontui ensimmäisen kerran 8.5.2024, ja 9.8.2024 mennessä se oli pitänyt yhteensä 15 kokousta.

Kaupungin koordinaatioryhmä linjasi tärkeimmät tilanteen johtamiseen ja hoitamiseen liittyvät toimenpiteet ja viestintään liittyvät asiat digijohtajan, KASKOn toimialajohdon sekä viestintäjohdon esittelystä. Ryhmä kokoontui 6.5.-6.8.2024 välisenä aikana 23 kertaa.

Valmisteluryhmän tehtävänä oli tilannekuvan ylläpito, asioiden valmistelu johdolle sekä kaupunkitason viestinnän johtaminen. Ryhmä kokoontui ensimmäisen kerran 4.5.2024 ja sen jälkeen lähes päivittäin 31.5.2024 saakka yhteensä 28 kertaa. Tämän jälkeen ryhmä kokoontui 10.7.2024 asti vielä yhdeksän kertaa.

Operatiivisen projektiryhmän tehtävänä oli työskennellä valmisteluryhmän ohjauksessa. Se huolehti tietomurron kohteiden ja vaikutusten arvioinnin toimeenpanon varmistamisesta sisältäen kaupungin ja ulkoisten resurssien koordinoinnin sekä viranomaisyhteistyön. Lisäksi ryhmän tehtävänä oli koostaa tilannekuvaa valmisteluryhmälle. Ryhmä laati myös viestintään liittyvät sisällöt valmisteluryhmän ohjeiden perusteella viestinnän ohjauksessa. Ryhmä kokoontui ensimmäisen kerran 6.5.2024 ja toukokuun aikana yhteensä kahdeksan kertaa.

Viestinnästä vastasi kaupungin kanslian puolesta viestintäjohtaja sekä KASKOn osalta viestintä- ja markkinointipäällikkö. He muodostivat yhdessä viestintähenkilöiden kanssa koordinaatioryhmän, joka huolehti tehostetun viestinnän toteuttamisesta. Viestinnän kokouksissa käytiin läpi muun muassa median haastattelupyynnöt, kysymys- ja vastausosion päivitys, uutisointi, sisäinen viestintä ja henkilöstön tietoturvaan liittyvä koulutus.

Kaupungin tasolla tapahtumaa käsiteltiin myös viestintä-, tietoturva- ja tietosuojaryhmien kokouksissa sekä kaupunginhallituksen ja kaupunginvaltuuston kokouksien yhteydessä. Asiaa käsiteltiin myös kasvatus- ja koulutuslautakunnassa.

1.4 Viestintä tietomurrosta

Helsingin kaupunki tiedotti tietomurrosta 30.4.2024 julkaisemalla kaupungin sisäisessä intrassa häiriöbannerin heti asian paljastuttua sekä käynnisti kaupungin kansliasta johdetut tehostetut viestintätoimet. Kaupungin intrassa julkaistiin *häiriöbanner*-viesti, jossa kerrottiin tilanteesta ja lisäksi asian kehittymisestä tiedotettiin sähköpostilla toimialojen johtoryhmille.

Iltalehti uutisoi ensimmäisenä tietomurrosta 1.5.2024 klo 20:31 otsikolla ”Epäily: Venäjältä murtauduttu Helsingin tietoverkkoon – Henkilötietoja vaarassa.”[10] Uutinen levisi laajasti eri medioissa.

Helsingin kaupunki julkaisi mediatiedotteen 2.5.2024 klo 13:25 ja kertoi verkkosivuillaan kasvatuksen ja koulutuksen toimialaan kohdistuneesta tietomurrosta.[11] Tiedotteessa kaupunki kertoi, että tietomurron tekijä on saanut haltuunsa kaupungin kaikkien työntekijöiden käyttäjätunnukset ja sähköpostiosoitteet sekä kasvatuksen ja koulutuksen toimialan oppijoiden, huoltajien ja henkilöstön henkilötunnuksia sekä osoitetietoja. Tiedot välitettiin myös kaupungin perusopetuksen ja toisen asteen oppijoille ja huoltajille Wilmassa sekä toimitettiin päiväkoteihin eteenpäin lähetettäväksi. Lisäksi uutinen julkaistiin kaupungin intranetissä.

Koska viestiminen tietoturvaloukkauksesta ja vastuu lisätietojen antamisesta on lain nojalla rekisterinpitäjällä eli Helsingin kaupungilla, sen hallituksella ja lautakunnilla, kaupunki otti vastuun viestinnän koordinoinnista. Tietomurron kohteena olevia uhreja ei voitu yksilöidä, joten kaupunki ilmoitti tietosuojavaltuutetun toimistolle 8.5.2024 että rekisteröityjä tullaan informoimaan julkisella tiedoksiannolla.[12]

Kyberturvallisuuskeskus perusti 7.5.2024 tietomurtoon keskittyvän sisäisen keskusteluryhmän, johon osallistuivat tietomurtoa tutkiva yritys sekä keskeiset viranomaiset. Ryhmää käytettiin tutkinnan koordinointiin ja viestinnän tukemiseen.

Helsingin kaupunki kertoi tietomurrosta julkisuuteen seuraavan kerran *Helsinki-kanavalla*[13] 13.5.2024 pidetyssä tiedotustilaisuudessa, jossa olivat läsnä Helsingin kaupungin sekä Kyberturvallisuuskeskus ja poliisin edustajat. Paikalla oli viisi median edustajaa. Verkon kautta tilaisuutta seurasi suorana arviolta 1 300 katsojaa ja tallenne jäi katsottavaksi kaupungin nettisivulle.

Tilaisuudessa kerrottiin tietomurron selvitystyön tuloksista ja annettiin uhreille ohjeita omien henkilötietojen suojaamiseksi. Helsingin kaupunki kertoi, että se toteuttaa rekisteröityjen informoinnin julkisena tiedonantona verkko-osoitteessa *hel.fi/tietomurto*. Sivustolla oli tietoa selvitystyön etenemisestä, vastauksia kysymyksiin ja ohjeita rekisteröidyille.[14]

Tilaisuudessa poliisi ilmoitti, että tapauksen asianomistaja on Helsingin kaupunki, eikä yksittäisten kansalaisten kannata ottaa yhteyttä poliisiin oman rikosilmoituksen tekemistä varten. Samalla poliisi ilmoitti tutkivansa tapausta törkeänä tietomurtona ja lupasi tiedottaa lisää myöhemmin.

---

[10] Iltalehden uutinen 1.5.2024. 26.2.2025 https://www.iltalehti.fi/kotimaa/a/8d3e0f58-76fe-42e3-acb8-41f51eb70fac

[11] Helsingin kaupunki: Julkinen tiedote kasvatuksen ja koulutuksen toimialan tietomurron mahdollisille kohderyhmille. 1.9.2024 https://www.hel.fi/fi/paatoksenteko-ja-hallinto/kaupungin-organisaatio/toimialat/keskushallinto/kasvatuksen-ja-koulutuksen-tietomurto/julkinen-tiedote-kasvatuksen-ja-koulutuksen-toimialan-tietomurron-mahdollisille-kohderyhmille

[12] Tietosuoja-asetus 34, artikla 3c.

[13] Kanava, jossa Helsingin kaupunki lähettää suoria lähetyksiä sekä julkaisee videoita ja podcasteja.

[14] Helsingin kaupunki. 1.9.2024 https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto

KASKOssa työskenteleviä esihenkilöitä informoitiin Teams-kokouksessa. Kansliapäällikkö lähetti sähköpostin kaupungin henkilöstölle. Wilman kautta viestittiin kaupungin perusopetuksen ja toisen asteen huoltajille, oppijoille sekä henkilöstölle. Varhaiskasvatuksessa viesti välitettiin sähköpostilla perheille.

Helsingin Poliisi tiedotti 13.5.2024 klo 14:26, että se tutkii Helsingin kaupungin tietoverkon laajaa tietomurtoa. Poliisi tutkii tapausta tällä hetkellä törkeänä tietomurtona.

Tietosuojavaltuutettu tiedotti 14.5.2024 tietomurtoon liittyvistä selvitystoimista ja antoi ohjeita tietomurron uhreille.

Helsingin kaupungin kasvatuksen ja koulutuksen asiakkaat edustavat yli sataa eri kieliryhmää.[15] Oppijoille ja heidän huoltajilleen tiedotettiin aluksi suomeksi, ruotsiksi ja englanniksi. Myöhemmin lisättiin tiedotusta mm. venäjäksi, arabiaksi ja somaliksi.

Peruskoulujen huoltajatiedote lähetettiin Wilman kautta ja varhaiskasvatuksen tiedote päiväkodin johtajien kautta huoltajille. Lukioiden ja Stadin Ammattiopiston tiedotteet lähetettiin oppijoille ja huoltajille Wilman kautta.

Opettajien Digipolku-ohjeistukseen lisättiin tietoa tietomurroista. Kaupunki ei tehnyt erillistä kohdennettua ja ikätason mukaista viestintää alaikäisille rekisteröidyille.

Kaupunki avasi huoltajille ja oppijoille puhelinpalvelukanavan ja erillisen sähköpostiosoitteen. Tietopyyntöjä varten luotiin sähköinen lomake, joka ohjautui suoraan tietomurtoon liittyvään sähköpostiin.

Poliisi tiedotti 17.5.2024, että Keskusrikospoliisi ja Helsingin poliisi tutkivat yhteistyössä kaupungin järjestelmiin kohdistunutta törkeää tietomurtoa. Poliisi ohjeisti, että jokaisen, joka epäilee omien tietojensa vaarantuneen, on hyvä tehdä toimia oman identiteetin suojaamiseksi. Poliisi kertoi, että viestinnän osalta poliisilla on vastuu rikostutkintaan liittyvästä tiedottamisesta ja Helsingin kaupunki rekisteripitäjänä kertoo, millaisia tietoja järjestelmistä on päässyt vuotamaan ja keitä henkilöitä tämä koskee.

Helsingin kaupunki julkaisi mediatiedotteen 21.5.2024, jossa kerrottiin selvitystyön etenemisestä ja siitä, että tietomurron mahdolliset kohderyhmät ovat laajentuneet. Samalla kerrottiin, että tekijä on saattanut saada haltuunsa aiemmin arvioitua laajemmin tietoja kasvatuksen ja koulutuksen palveluja käyttäneistä henkilöistä. Sen hetkisen arvion mukaan tietomurto koski noin 150 000 oppijaa ja heidän huoltajiaan. Vastaava viesti toimitettiin perusopetuksen ja toisen asteen Wilmassa sekä päiväkodeissa viesti välitettiin huoltajille. Lisäksi viesti välitettiin yksityisille päiväkodeille sekä yksityisille ja valtion kouluille. Torstaina 23.5.2024 kaikille kaupungin esihenkilöille lähetettiin kansliapäällikön viesti koskien tilannetta. Tietomurron kesäaikaisesta tiedottamisesta välitettiin viesti Wilmassa sekä päiväkodeissa 30.5.2024.

Kaupunki julkaisi 21.5.2024 sivulla *hel.fi/uutiset* asiantuntijan antamat ohjeet siitä, miten toimia tietomurron keskellä ja kertoi, että tietomurron tekijä on saattanut saada haltuunsa tietoja kaikista helsinkiläisistä oppivelvollisista. Samana päivänä kaupunki tiedotti sosiaalisen median X-palvelussa, että ajantasainen tieto tietomurtoon liittyvistä asioista löytyy hel.fi/tietomurto -sivulta.

Sisäistä viestintää jatkettiin ja esihenkilökirje lähetettiin 23.5.2024 tiedoksi sähköpostitse.

KASKOn henkilöstölle kerrottiin intranetin tietoturvan tehostetusta valvonnasta.

---

[15] Vieraskielinen väestö: kieliperusteisen tilastoinnin ongelmia ja ratkaisuvaihtoehtoja. 15.1.2025 https://kaupunkitieto.hel.fi/fi/vieraskielinen-vaesto-kieliperusteisen-tilastoinnin-ongelmia-ja-ratkaisuvaihtoehtoja

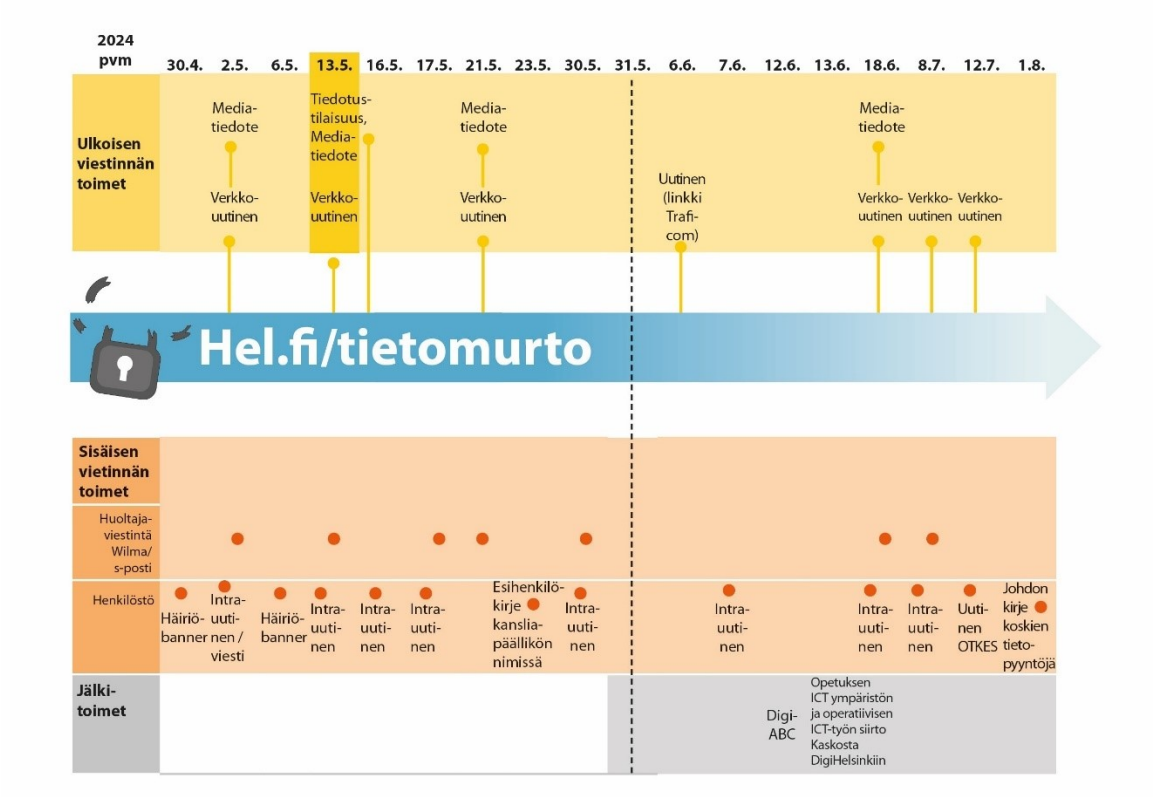
Turvakiellon alaisia rekisteröityjä ei pystytty tavoittamaan välittömästi tietomurron tapahduttua. Turvakielto on poikkeuksellinen toimi, jolla rajoitetaan yhteystietojen luovuttamista väestötietojärjestelmästä. Henkilöllä, jolla on turvakielto, tieto osoitteesta ja kotikunnasta voidaan luovuttaa vain sellaisille viranomaisille, jotka saavat käsitellä turvakiellon alaisia tietoja.

Kaupunki julkaisi 6.6.2024 jälkiviestinnän toimenpiteinä uutisen, jossa kerrottiin Liikenne- ja viestintävirasto Traficomin henkilötietojen suojaamisohjeista somalin, arabian ja venäjän kielillä. Kaupunki tiedotti 18.6.2024, ettei kaupunkiin kohdistunut tietomurto ole enää laajentunut. Turvaa yhteinen tietomme -tallenne julkaistiin kaupungin intranetissä 7.6.2024.

Verkkouutisessa kerrottiin 8.7.2024, että tarkennettua tietoa tietomurrosta on annettu tietosuojavaltuutetulle. Kaupunki tiedotti 12.7.2024 että Onnettomuustutkintakeskuksen yhteyteen on perustettu riippumaton tutkintaryhmä, joka aloittaa tutkinnan Helsingin kaupunkiin kohdistuneesta tietomurrosta. Vastaavat viestit toimitettiin perusopetuksen ja toisen asteen Wilmassa sekä päiväkodeissa viesti välitettiin huoltajille.

Sisäistä viestintää jatkettiin kesäkuussa intranet-uutisten sekä DigiABC-koulutuksen päivityksen muodossa.

Kaupunki julkaisi 17.12.2024 verkkouutisen tietomurron tilanteesta ja välitti myös tämän viestin perusopetuksen ja toisen asteen Wilmassa. Viesti välitettiin myös varhaiskasvatuksessa.



Kuva 2: Helsingin kaupungin viestintätoimet tietomurrosta.

1.5 Hälytykset ja pelastustoimet

Vaikka hyökkääjä pyrki toimimaan mahdollisimman huomaamattomasti hyödyntämällä Windows-käyttöjärjestelmän sisäisiä komentoja ja työkaluja, toiminta aiheutti kuitenkin hälytyksiä sekä palvelinten että verkkolaitteiden lokeihin. Hyökkääjän noudattaman LOTL-tekniikan (Living Off The Land[16]) tunnistaminen on hankalaa, koska siinä hyödynnetään laillisia ohjelmistoja ja tavanomaisia järjestelmäkomponentteja, joiden käyttö ei yleensä johda hälytyksiin.

Tikettijärjestelmän virheen vuoksi haittaohjelmien torjuntaohjelman hälytys 25.4.2024 ei mennyt perille KASKOlle. Se välitettiin eteenpäin 29.4.2024, mutta ilmoitukseen ei reagoitu. Vasta uudet hälytykset aamuyöllä 30.4.2024 johtivat torjuntavasteen käynnistymiseen KASKOssa ja DigiHelsingissä.

[16] Living Off The Land on kyberhyökkäystekniikka, jossa käytetään haittaohjelmien sijaan mahdollisimman paljon kohdejärjestelmän omia työkaluja ja resursseja haitallisiin tarkoituksiin.

Hälytys merkitty keltaisella

Ajankohta		Tapahtuma	Hyökkääjä	Helsingin kaupunki	KASKO	DigiHelsinki Oy	Kaupalliset palveluntarjoajat	Kyberturvallisuuskeskus	Tietosuojavaltuutetun toimisto	Helsingin poliisi	Keskusrikospoliisi
2014		Cisco ASA 5515 VPN-reititin hankitaan Opetusvirastoon (KASKOn edeltäjä) etäyhteyksien toteuttamista varten.			X						
2016		Viimeinen tietoturvapäivitys VPN-reitittimelle KASKOn toimesta, ohjelmisto vuoden 2015 tasolla.			X						
2017		VPN-reitittimen ylläpidosta vastanneet henkilöt lähtevät KASKOlta.			X						
2018		ASA 5515:n rinnalle hankitaan uudempi ASA 5545, mutta sitä ei ehditä ottaa käyttöön ennen kuin laitteesta vastannut työntekijä lähtee KASKOlta.			X						
2019		Hyväksytään hankintapäätös uusien VPN-laitteiden hankkimiseksi vanhojen korvaajaksi, mutta laitteita ei kuitenkaan hankita.		X	X						
2020		VPN-reitittimen käyttäjien siirto alkaa uuteen DigiHelsingin etäkäyttöpalveluun.			X	X					
29.2.2024		Väsytyshyökkäys (brute force) KASKOn verkkoon 29.2.-4.4.2024.	X								
31.3.2024		Dustin Oy päivittää etäyhteydellä VPN-reitittimeen uuden varmenteen, joka on taas voimassa vuoden.			X	X	X				
8.4.2024		Väsytyshyökkäys 8.4-12.4.2024, jolla kerätään teknistä tietoa KASKOn verkosta ja vanhentuneesta VPN-reitittimestä.	X								
14.4.2024	20:14	VPN-reititin kaatuu haavoittuvuuden hyväksikäytön seurauksena. Asiaa ei tutkita sen tarkemmin.	X		X						
18.4.2024	11:17	Hyökkääjän todennäköisesti ensimmäinen kirjautuminen VPN-reitittimelle.	X								
23.4.2024	11:14	Hyökkääjä kartoittaa KASKO:n IT-infrastruktuuria, josta syntyy ilmoituksia lokeihin, mutta aktiivista valvontaa ei ole eikä hälytystä synny.	X								
25.4.2024	13:17	Hyökkääjä saa ensimmäisen kerran jalansijan KASKOn sisäverkkoon.	X								
	13:40	Kirjautumisista syntyy ensimmäinen matalan tason tietoturvahälytys klo 13:40 ja korkeamman tason hälytys klo 13:59 sekä tämän jälkeen hälytyksiä yhdeksältä eri laitteelta.				X	X				
	15:07	Hyökkääjän ensimmäinen kirjautuminen KASKOn palvelimelle etätyöpöytäyhteydellä.	X								
	17:22	Haittaohjelmien torjuntaohjelma hälyttää epäonnistuneista kirjautumis-yrityksistä. DigiHelsingin alihankkija avaa havainnoistaan keskimääräisen vakavuustason tiketin. Tiketti ohjautuu klo 18:36 toiselle alihankkijalle, joka hoitaa Helpdeskin 1-tason ja muiden palveluiden integraatioita eri toimittajille.					X				
	18:40	Hyökkääjä on saanut haltuunsa pääkäyttäjän oikeudet kahteen Microsoft Windows-toimialueeseen, virtuaalipalvelinympäristön hallintapalvelimeen sekä varmuuskopiointijärjestelmään.	X								
26.4.2024	2:54	Hyökkääjä käynnistää ensimmäisen 1,03 Gt tiedostosiirron ulkomailla sijaitsevalle palvelimelle. Siirto kestää kolme minuuttia.	X								
27.4.2024	0:01	Hyökkääjä käynnistää kolme laajempaa tiedostosiirtoa ulkomailla sijaitsevalle palvelimelle.	X								
29.4.2024	11:34	25.4. klo 17:22 lähetetty hälytys (tiketti) havaitaan ja saadaan käsittelyyn. Teknisen virheen vuoksi hälytys on jäänyt on hold -tilaan.				X	X				
	11:54	KASKO saa ensimmäisen hälytyksen mahdollisesta tietomurrosta DigiHelsingin helpdesk-palvelusta koskien 25.4. tapahtuneita kirjautumis- ja salasanojen tietomurtoyrityksiä.			X	X	X				

Hälytys merkitty keltaisella

Ajankohta		Tapahtuma	Hyökkääjä	Helsingin kaupunki	KASKO	DigiHelsinki Oy	Kaupalliset palveluntarjoajat	Kyberturvallisuuskeskus	Tietosuojavaltuutetun toimisto	Helsingin poliisi	Keskusrikospoliisi	Suojelupoliisi
30.4.2024	1:30	Hyökkääjä käynnistää väsytyshyökkäyksen 165 tietokoneelle päästäkseen kahdelle muulle Helsingin kaupungin toimialueelle. Klo 3:10 hyökkääjä yrittää murtautua Helsingin kaupungin muiden toimialojen verkkoihin, mikä aiheuttaa hälytyksiä haittaohjelmien torjuntaohjelmistossa.	X									
	9:30	Aamuyöllä tapahtuneita hälytyksiä käsitellään DigiHelsingin ja KASKOn säännöllisessä kokouksessa. Epäily tietomurrosta varmistuu ja tieto sen vakavuudesta alkaa selvitä.			X	X						
	13:00	Aamupäivän tietojen perusteella käynnistetään MIM-häiriönhallintaryhmän toiminta ja ensimmäinen kokous järjestetään klo 13:00.		X	X	X						
	13:40	Päivän aikana tehdyn tutkinnan perusteella varmistuu, että hyökkääjä on päässyt KASKOn sisäverkkoon Cisco ASA 5515 VPN-reitittimeltä, joka irrotetaan verkosta.			X	X						
		Helsingin kaupunki tekee viranomaisilmoitukset Kyberturvallisuuskeskukselle ja Tietosuojavaltuutetun toimistolle.		X	X			X	X			
		Verkon ja palvelinten kriittisiä salasanoja aletaan vaihtamaan uusiin.			X	X						
1.5.2024		Rikosilmoitus poliisille tehtiin 1.5. aamulla.								X		
		KASKOn verkosta eristetään tai suljetaan palvelimia, joille hyökkääjän tiedetään murtautuneen. Salasanojen vaihtoprojekti jatkuu.			X	X						
2.5.2024		Tietojen vaihto Traficomin Kyberturvallisuuskeskuksen ja KASKOn välillä alkaa.			X			X				
3.5.2024		Ulkopuolinen palvelutoimittaja aloittaa tietoturvaloukkauksen hallinta- ja tutkintatoimenpiteet Helsingin kaupungin toimeksiannosta.			X		X					
		Tietomurron kohteeksi joutunut verkkolevy irrotetaan KASKOn verkosta ja siirretään toiseen, turvalliseksi varmistettuun palvelimeen.			X	X						
		Suojelupoliisi ottaa yhteyttä Helsingin kaupunkiin.			X							X
4.5.2024		Valmisteluryhmä aloittaa toimintansa.		X	X	X						
		Ulkopuolinen palvelutoimittaja käynnistää 24/7 rajoitetun tietoturvavalvomo-toiminnan (SoC, Security Operation Center).			X		X					
8.5.2024		Varmuuskopiointijärjestelmä havaitaan saastuneeksi ja käyttökelvottomaksi, mutta sille ei ole tarvetta.			X	X						
9.5.2024		Kyberturvallisuuskeskus aloittaa tapahtuneesta erityisseurannan.			X		X	X		X		
13.5.2024		Helsingin kaupunki järjestää avoimen tiedotustilaisuuden.		X	X			X		X		
31.5.2024		Verkkolevy toiminnassa uudella alustalla ja avautuu takaisin henkilökunnan käyttöön.		X	X							

Kuva 3. Aikajana tietomurron etenemisestä ja siitä toipumisesta.

Tietotekniset pelastustoimet käynnistyivät varsinaisesti 30.4.2024 klo 13:40, kun KASKOn ja DigiHelsingin henkilökunta sulki pääsyn VPN-reitittimelle. Asiantuntijat estivät ensin laitteen käytön ja sen jälkeen laite irrotettiin fyysisesti verkosta. Sähköä ei kuitenkaan katkaistu, jotta laitteen RAM-muistissa[17] olevat tiedot saatiin säilymään tarkempaa tutkintaa varten. Laitteesta löytyneiden loki- ja muiden digitaalisten jälkien tutkinnassa käytettiin apuna valmistajan ulkomailla sijaitsevia asiantuntijapalveluita.

KASKOn sisäverkon ylläpitäjiä kehotettiin 30.4.2024 klo 17:15 vaihtamaan salasanansa. Samalla aloitettiin palvelinten paikallisten ja teknisten käyttäjätunnusten salasanojen vaihto, joka jatkui 1.5.2024. Samana päivänä KASKO ja DigiHelsinki alkoivat eristää ja sulkea tietomurron kohteeksi joutuneita palvelimia.

[17] RAM-muisti (Random-Access Memory) on IT-laitteen sisäinen muisti.

Helsingin kaupunki teki tietomurtoepäilyn paljastuttua ilmoitukset seuraaville viranomaisille:

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle 30.4.2024
- Tietosuojavaltuutetun toimistoon 30.4.2024
- Rikosilmoitus poliisille 1.5.2024, joka kirjattiin poliisin järjestelmiin 30.4. klo 4:26 käynnistyneenä törkeänä tietomurtona.

Ilmoitusten tekohetkellä ei ollut käsitystä tietomurron laajuudesta tai vakavuudesta. Ilmoituksissa kuvattiin tietomurron tekijän saaneen haltuunsa käyttäjien ja ylläpidon verkkotunnuksia sekä sähköpostiosoitteita.

Helsingin kaupungilla tapahtunut tietoturvaloukkaus tuli ensimmäistä kertaa Kyberturvallisuuskeskuksen tietoon 30.4.2024 klo 23:30. Helsingin kaupunki teki ensi-ilmoituksen kyberturvallisuuskeskuksen verkkosivustolla olevalla "Ilmoita tietoturvaloukkauksesta"-lomakkeella. Ilmoitukseen vastattiin ensimmäisen kerran 12 tunnin kuluttua ensi-ilmoituksesta eli 1.5.2024 Kyberturvallisuuskeskuksen päivystäjän toimesta. Kyberturvallisuuskeskus aloitti asiaa koskevan tiedonvaihdon 1.5.2024. Asia otettiin käsittelyyn Kyberturvallisuuskeskuksessa sisäisesti ensimmäisen kerran 1.5.2024 klo 19:30.

Kyberturvallisuuskeskuksen vastaanottamassa ensi-ilmoituksessa kerrottujen tietojen perusteella ilmoitettu poikkeama ei vaikuttanut sen suorittamassa tapauksen vakavuusarviossa sellaiselta, että se olisi edellyttänyt Kyberturvallisuuskeskukselta välittömiä normaalista prosessista poikkeavia toimenpiteitä. Ilmoituksen tietojen perusteella tilanne vaikutti olevan Helsingin kaupungilla hyvin hallinnassa: muun muassa tapausta selvittämään oli hankittu ulkopuolinen kumppani ja tietoturvapoikkeamaan liittyviä rajoittamistoimenpiteitä oli jo tehty.

Kyberturvallisuuskeskus aktivoi Helsingin kaupungin tietoturvapoikkeaman koordinaation eri viranomaisten ja muiden tahojen kesken.

Tietosuojavaltuutetun toimisto otti vastaan tehdyn tietoturvapoikkeamailmoituksen ja aloitti sen käsittelyn normaalin tutkintaprosessinsa mukaisesti. Tietosuojavaltuutetun toimisto ei toteuttanut välittömiä toimenpiteitä, mutta pyysi täydennystä KASKOn toimittamaan materiaaliin. KASKO vastasi tietosuojavaltuutetun lisäpyyntöihin 9.5.2024, 5.6.2024 ja 8.7.2024.

Helsingin poliisin tutkinnanjohtaja otti yhteyttä KASKOon 2.5.2024.

Helsingin kaupunki kysyi ulkopuolista apua tietoturvaloukkauksen hallinta- ja tutkintatoimenpiteisiin 30.4.2024 tunnetulta kaupalliselta toimijalta, mutta sillä ei ollut valmiutta toimittaa palvelua Suomesta. Sen jälkeen KASKO kääntyi Elisa Santa Monican puoleen, joka aloitti tietomurron tutkintatoimenpiteet 3.5.2024 klo 8:00. Se käynnisti ympärivuorokautisen tietoturvavalvomon 4.5.2024 klo 17:00 ja sai alustavasti varmistettua, että hyökkäys on kohdistunut vain KASKOn IT-ympäristöön eikä hyökkääjä ollut päässyt muiden toimialojen IT-ympäristöihin.

Elisa Santa Monican päätti tietomurtotutkinnan 11.9.2024, jonka jälkeen se toimitti Helsingin kaupungille raportin 7.10.2024. Yhteistyö jatkui tietoturvapalvelujen tuottamisella Helsingin kaupungille.

Suojaustoimena otettiin 2.5.2024 käyttöön tekninen maasuojaus (geoblokkaus), joka rajoitti kirjautumisia Helsingin kaupungin palveluihin Suomen rajojen ulkopuolelta.

KASKO irrotti hyökkäyksen kohteeksi joutuneen verkkolevyn ja esti sen käytön 3.5.2024. Tässä yhteydessä verkkolevy siirrettiin tietomurron kohteeksi joutuneesta palvelimesta uuteen, tietoturvan osalta varmistettuun alustaan, jossa asiantuntijat pääsivät tutkimaan sitä.

Suojelupoliisi otti yhteyttä Helsingin kaupunkiin 3.5.2024 ja pyysi lisätietoja, koska mediassa oli nostettu esille mahdollinen kytkentä Venäjään.

Palvelinten ja verkon pääkäyttäjien ja palvelutunnusten salasanojen vaihtaminen käynnistyi pääkäyttäjien toimesta 3.5.2024. Samassa yhteydessä uusittiin palvelinten aitouden todistavat varmenteet ja vanhat varmenteet poistettiin käytöstä.

Tekniikan ja viestinnän toimet tietomurron hallitsemiseksi

Tietomurron tutkinnassa auttava Elisa Santa Monica käynnisti selvityksen (tietomurtotutkintapalvelu), jonka tehtävänä oli tunnistaa hyökkääjän pääsyn laajuus, estää hyökkäyksen leviäminen uusille laitteille sekä mahdollisen aktiivisen jalansijan poistaminen ympäristöstä. Sen jälkeen keskeinen toimenpide oli varmistaa, ettei ympäristöön ole jätetty takaportteja, joiden avulla hyökkääjä pystyisi palaamaan takaisin.

Yritys käynnisti ympärivuorokautisen tietoturvavalvomo-toiminnan (Security Operation Center, SoC), jonka toimintaa laajennettiin 14.5.2024 asentamalla KASKOn palvelimiin ja laitteisiin kehittyneemmät päätelaitevalvontasensorit tietoturvapoikkeamien havaitsemiseksi.

Varotoimenpiteenä sammutettiin kahdesta eri AD-toimialueesta yksi domain controller -palvelin, jotta käyttäjähakemiston tiedot saatiin suojattua.

Pääkäyttäjille otettiin käyttöön uusia, varmasti haittaohjelmista vapaita työasemia. Tietomurron kohteeksi joutuneen verkkolevyn tiedostojen siirtoa toiselle palvelimelle alettiin valmistella 6.5.2024.

Laitteista, jotka eivät enää olleet verkossa tai etähallinnassa, alettiin ottaa levykuvia 9.5.2024 tietomurron laajuuden selvittämiseksi.

Viestinnän ensitoimenpiteinä Helsingin kaupunki laittoi 30.4.2025 välittömästi *häiriö-bannerin* intranettiin ja tiedotti julkisesti 2.5.2025 tietomurrosta.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus antoi myös tutkinta-apua muun muassa tietoturvatutkinnan kannalta kriittisen aineiston keräämiseen liittyen. Se avusti Helsingin kaupunkia ja sen käyttämää tietoturvapalvelujen tarjoajaa tietomurron tilanteen ja laajuuden selvittämisen kannalta kriittisen rikosteknisen tutkinta-aineiston keräämisessä tietomurron kohteena olevilta palvelimilta. Lisäksi Kyberturvallisuuskeskus teki tutkinnan alkuvaiheessa tilanteen olleessa vakavimmillaan myös omaa analyysia tapahtumasta.

Tietopyyntöihin vastaaminen

Helsingin kaupunki alkoi 2.5.2024 suunnitella palvelua, joka pystyisi vastaamaan verkkolevyllä sijainneiden henkilötietojen tarkastuspyyntöihin. Koska sopivaa valmisohjelmaa ei löytynyt, kaupungin kanslian digitalisaatioyksikköön kuuluva Data ja uudet teknologiat -tiimi päätyi rakentamaan niitä varten erillisen järjestelmän.

Kaupunki avasi 13.5.2024 nettisivullaan verkkolomakkeen, jolla vahvasti tunnistettu käyttäjä pystyi jättämään omia ja huollettavien tietoja koskevan tarkastuspyynnön. Sen jälkeen tehtävään nimetyt henkilöt etsivät asiakirjoista tarkastettavien henkilöiden tiedot henkilö- sekä oppilastunnusten perusteella. Tulokset lähetettiin pyytäjälle joko sähköisesti turvapostilla, perinteisellä kirjepostilla tai jätettiin noudettavaksi kirjaamoon riippuen siitä, miten pyytäjä oli toivonut vastaanottavansa asiakirjat.

Haku rajoittui henkilö- ja oppilastunnuksiin, sillä pelkällä nimellä haettaessa on mahdotonta erotella saman nimisiä henkilöitä toisistaan. Lisäksi tiedettiin, että valtaosassa henkilötietoja sisältävistä asiakirjoista oli jokin näistä kolmesta yksilöivästä tunnisteesta. Täysin vapaa tekstihaku nimen, osoitteen tai puhelinnumeron perusteella olisi lisännyt riskiä henkilötietojen luovuttamisesta väärälle henkilölle.

Tietomurron kohteena ollut verkkolevy kopiointiin DigiHelsingin palveluntarjoajan konesalissa sijaitsevalle verkkolevylle 19.5.2024.

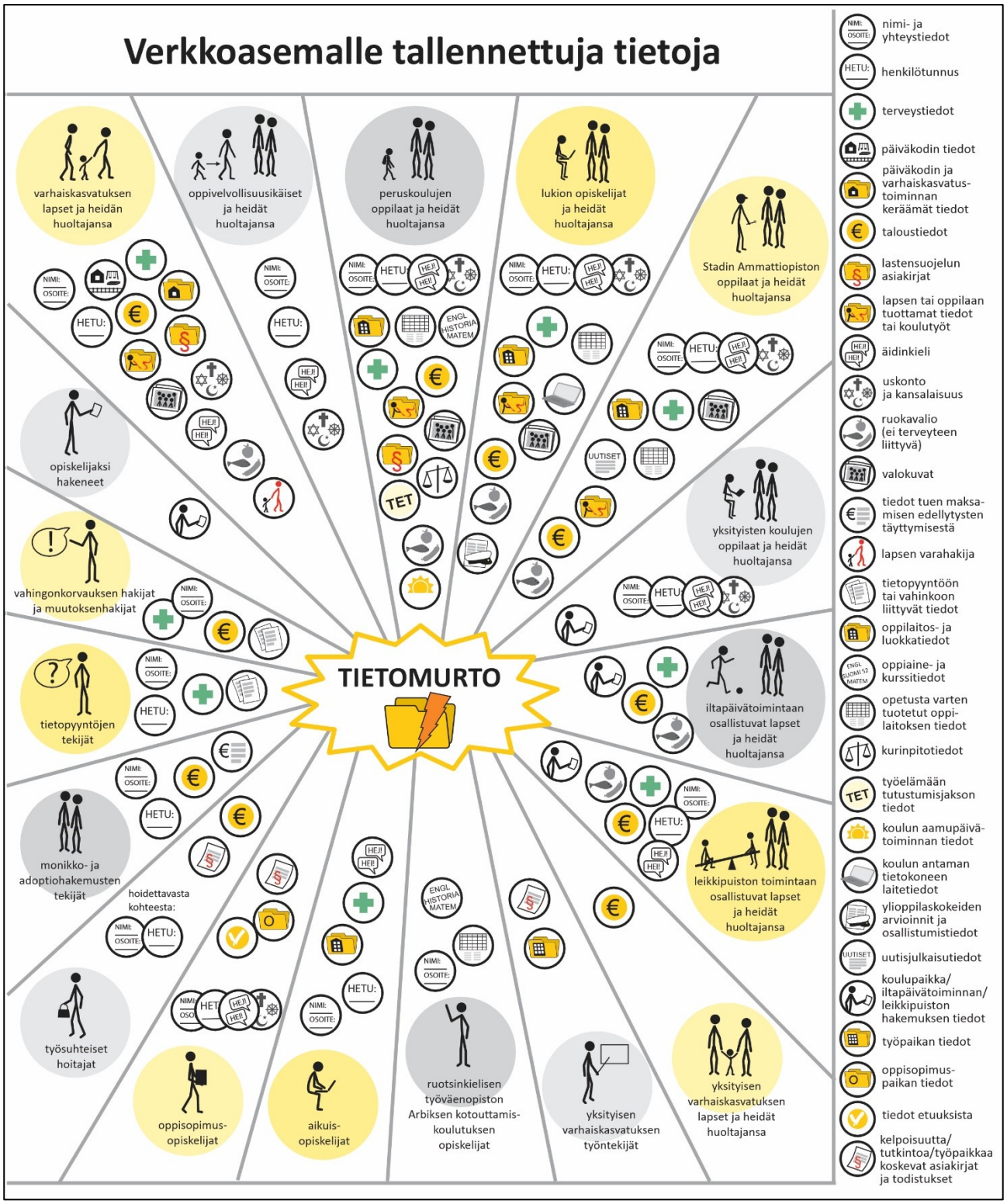
Uusi verkkolevy saatiin teknisesti toimintaan ja takaisin henkilöstön käyttöön 31.5.2024, kun sen tiedostot oli tarkistettu ja varmistettu turvallisiksi kahdella tietoturvaohjelmalla mahdollisten haittaohjelmien löytämiseksi. Käyttäjiä ohjeistettiin, ettei tiedostoja saa poistaa eikä verkkolevylle tallentaa uusia tiedostoja. Mahdolliset uudet tiedostot tuli tallentaa henkilökohtaiselle H: -asemalle.

1.6 Seuraukset

Tietomurron seurauksena hyökkääjän haltuun päätyi suuri määrä tietoa AD-käyttäjätietokannasta sekä verkkolevyltä. Tiedoissa oli mukana henkilötietoja ja osa niistä kuuluu erityisiin henkilötietoryhmiin[18] tai olivat muutoin salassa pidettäviä.

Tietomurron aineistossa oli satoja tuhansia ihmisiä koskevia tietoja. Osa näistä liittyi KASKOn tai Helsingin kaupungin henkilökuntaan, osa oppilaisiin ja heidän huoltajiinsa. Lisäksi verkkolevyn asiakirjoissa oli muiden välillisesti tai suoraan kaupungin kanssa asioineiden henkilöiden, yritysten ja muiden yhteistyötahojen tietoja.

[18] Erityisillä henkilötiedoilla tarkoitetaan tietoja, joista ilmenee henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveydentila, seksuaalinen suuntautuminen tai käyttäytyminen geneettisiä sekä biometrisia tietoja, joita voidaan käyttää henkilön tunnistamiseen.



Kuva 4. Verkkolevylle tallennettuja tietosisältöjä henkilöryhmittäin.

Verkkolevyn sulkeminen vaikeutti KASKOn arjen toimintaa erityisesti toukokuussa 2024. Useat KASKOn IT-infrastruktuurin hallintaan tai palveluiden tuottamiseen liittyvät tietojärjestelmät olivat poissa käytöstä, mikä vaikutti KASKOn sisäiseen toimintaan sekä asiakkaille tarjottavien palveluiden toimintaan myös vielä syksyllä 2024.

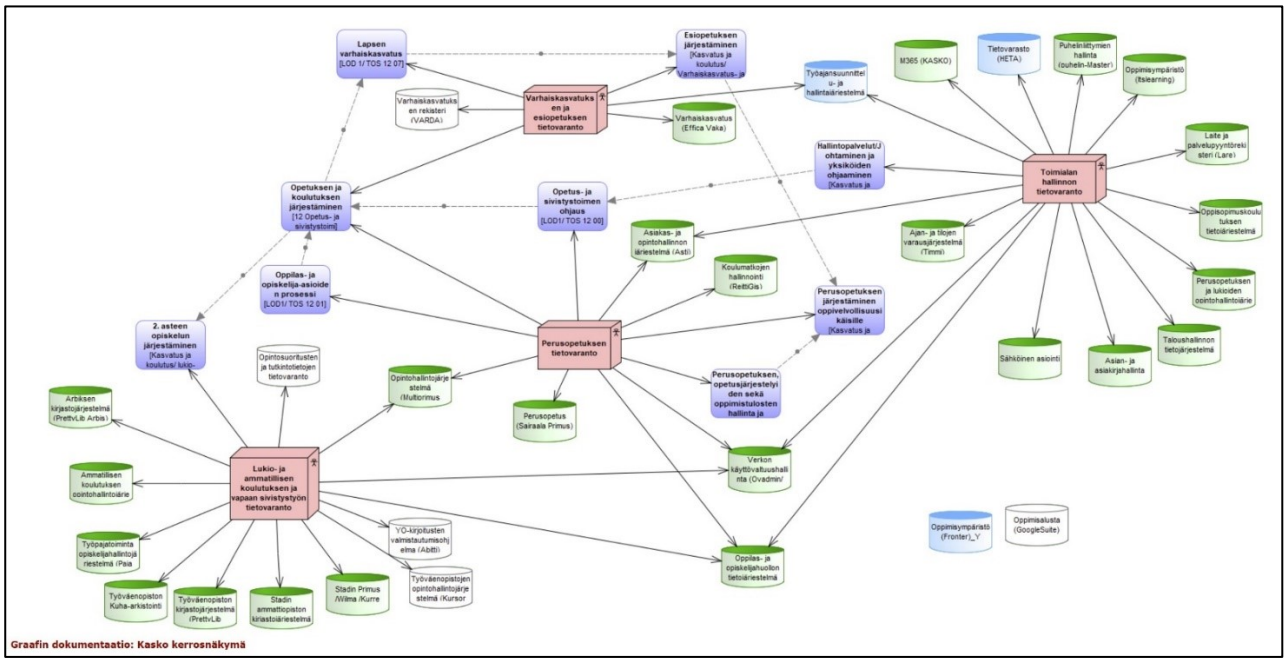
Tapahtuman selvittelystä ja korjaamisesta aiheutui Helsingin kaupungille merkittäviä kustannuksia. Tietomurron tutkimisesta ja palautumisesta aiheutuneet välittömät kustannukset touko-syyskuun 2024 aikana olivat noin 650 000 euroa. Sen lisäksi muun muassa uusien tietoturvapalveluiden käyttöönotosta aiheutui vähintään 400 000 euron kustannukset. Osan näistä investoinneista voidaan laskea olevan vanhentuneen IT-infrastruktuurin korjausvelkaa. Tapahtuman tutkinta ja sen perusteella käynnistettävät kehittämistoimenpiteet vaikuttavat myös muiden Helsingin kaupungin toimialojen suunniteltujen ICT-hankkeiden toteuttamiseen.

Lisäksi Helsingin kaupungin henkilöstö ja sen alihankkijoina toimivat IT-palveluiden tuottajat joutuivat etenkin touko-kesäkuussa tekemään huomattavan määrän ylitöitä. Näitä kustannuksia ei selvitetty tarkemmin tutkinnassa.

2 TOIMINTAYMPÄRISTÖ, LAITTEET JA JÄRJESTELMÄT

Helsingin kaupungilla on käytössä lähes 600 erillistä tietojärjestelmää. KASKOlla omia järjestelmiä on yhteensä noin 300. Järjestelmäkokonaisuus on muodostunut pitkän ajan kuluessa. Tällaisessa kokonaisuudessa tyypillisiä ongelmia ovat järjestelmien hajanaisuus, niiden välinen tietojen vaihto ja teknisen käyttöiän hallinta. Kokonaisuuden hahmottamista on vaikeuttanut lisäksi se, että tietojärjestelmien käyttöönottomenettelyt eivät ole aina vakioituja. Erityisesti suppeita ja vain tiettyihin tehtäviin varattuja tietojärjestelmiä tulee käyttöön ja niitä poistuu käytöstä osana normaalia toiminnan muuttumista, eivätkä nämä muutokset tule aina käsitellyksi tai dokumentoiduksi.

Helsingin kaupungin tietojärjestelmien arkkitehtuurikuvissa ei ollut kuvattuna tietomurron kohteeksi joutunutta verkkolevyä. Ilmeisesti verkkolevy on jäänyt puuttumaan kuvauksista joko siksi, ettei verkkolevyä ole pidetty tietojärjestelmänä tai siksi, että verkkolevyt ovat olleet jäämässä taka-alalle erilaisten pilvipalveluympäristöjen käyttöönotossa. Verkkolevy oli ennen koronaepidemiaa suuremmassa roolissa Helsingin kaupungin KASKOn toiminnassa. Sittemmin on siirrytty käyttämään enemmän Teamsia ja Office 365:ta, jotka koetaan verkkolevyä ketterämmiksi. Tämä suuntaus jatkui myös sen jälkeen, kun tietomurron kohteena ollut verkkolevy otettiin takaisin käyttöön.



Kuva 5. KASKOn tietojärjestelmäarkkitehtuurikuvaus. (Kuva: Helsingin kaupunki)

Helsingin kaupunki on siirtynyt Microsoftin tarjoamien M365-palvelujen käyttöön vaiheittain vuodesta 2022.[19] Käyttöönoton yhteydessä kaupungilla on alettu käyttämään yhä enemmän pilvipalveluja. Pilvipalveluiden käyttöönottoon on Helsingin kaupungin kansliapäällikön 12.10.2022 antamat ohjeet henkilötietojen käsittelystä.[20]

[19] Microsoftin M365-palvelujen käyttöönotto Helsingin kaupungilla. 26.2.2025 https://paatokset.hel.fi/fi/asia/hel-2022-012015

[20] Henkilötietojen ja salassa pidettävien tietojen maantieteellistä sijaintia ja siirtoa koskevat edellytykset. 26.2.2025 https://paatokset.hel.fi/fi/asia/hel-2022-012014?paatos=252eaeba-1bed-4edb-a7a7-a0b55ee0f9f2

Ahjo-järjestelmä[21] on Helsingin kaupungin asianhallintajärjestelmä, jonka kehittämisestä ja järjestelmäylläpidosta vastaa kaupunginkanslian hallinto-osaston hallintomenettely- ja esikuntayksikkö. Ahjoon kirjataan ja tallennetaan viranomaiselle vireille tulevat asiat ja asiakirjat sekä laaditaan ja tallennetaan yleishallinnolliset päätökset, kuten hankinta-asiat, virkojen täyttöasiat sekä taloudelliseen päätöksentekoon liittyvät asiat. Viranhaltijapäätöksiä on myös muissa Helsingin kaupungin tietojärjestelmissä, ja ne liittyvät erityislainsäädännön tai muun erityistehtävän hoitamiseen.

Päätöksen valmistelu toteutuu tavallisesti siten, että asiaa valmisteleva henkilö laatii asiakirjaluonnoksen ja oheisaineiston Word tai Excel-tiedostoina. Nämä tiedostot valmistelija tallentaa työstön ajaksi omassa käytössään olevalle verkkolevylle, pilvipalveluun tai yhteiskäyttöiselle verkkolevylle. Laaditun aineiston perusteella valmistellaan päätös asianhallintajärjestelmään liittämällä asiakirjoja tai kopioimalla niistä tekstejä päätösasiakirjaan.

Kuvatun työnkulun ongelmana on, että päätösasiassa asiakirjoja kopioituu useisiin tallennuspaikkoihin, joista vain varsinaisessa asianhallintajärjestelmässä on asian elinkaaren hallintaominaisuudet. Muissa tallennussijainneissa asiakirjojen elinkaaren hallinta edellyttää käyttäjän itsensä tekemiä toimenpiteitä, kuten tiedoston poistamista. Hallintoasian valmistelijoiden työskentelytapana on ollut jättää aiempia asiakirjoja verkkolevylle ja pilvipalveluun, koska niitä käytetään pohjina seuraavien asioiden valmistelussa.

Helsingin kaupungin tiedonohjaussuunnitelman mukaisesti osa päätöksistä on tehty asianhallintajärjestelmän ulkopuolella ja näitä päätösasiakirjoja on tallennettu verkkolevylle. Näin on käsitelty erityisesti työnantajatoimintaan liittyviä päätöksiä.

Tyypillisesti suurin osa laadittavista asiakirjoista on kuitenkin muuta kuin varsinaista päätöksentekoaineistoa. Tämä on tavallista tosiasiallisessa hallintotoiminnassa kuten opetustyössä. Tässä tarkoituksessa laaditulle aineistolle ei ole ollut systemaattista hallintaa ja säilytysympäristöä ja noudatetut käytännöt ovat vaihdelleet laatijoiden ja toimintayksiköiden, kuten koulujen tai päiväkotien välillä.

Helsingin kaupunki teki dokumentinhallintajärjestelmän hankintapäätöksen 8.11.2023. Päätöstä ei ole voitu toteuttaa, sillä markkinaoikeus kumosi 26.4.2024 hankintasopimuksen muotovirheen takia.

KASKOn keskeiset asiakastietojärjestelmät ovat Effica Vaka varhaiskasvatuksessa, MultiPrimus perusopetuksessa, lukioissa ja ammatillisessa opetuksessa, AURA oppilashuollossa perusopetuksessa ja lukioissa, AMMAURA oppilashuollossa ammatillisessa koulutuksessa sekä Wilma kodin ja koulun välisessä tietojen vaihdossa. Tietomurto ei välittömästi kohdistunut asiakastietojärjestelmien tietoaineistoihin, mutta tietomurron kohteena oli tiedostoja, jotka olivat esimerkiksi raportteja asiakastietojärjestelmien tiedoista tai valmisteluasiakirjoja asiakastietojärjestelmään tallennettavaksi. AURA ja AMMAURA on sittemmin korvattu Kanta-yhteensopivalla Apotilla.

2.1 Tietomurto VPN-reitittimelle

Tietomurto tehtiin Ciscon palomuurilaitteelle, joka on tyyppiä ASA 5515 (Adaptive Security Appliance). KASKOssa sitä käytettiin VPN-yhteyksiä vastaanottavana reitittimenä.[22] Etäyhteys

[21] Ahjo on asiakirjahallintajärjestelmä, jolla asiakirjat voidaan ohjata organisaatiossa oikeille toimijoille.

[22] VPN-reititin on laite, johon etäkäyttäjät ottavat salatun yhteyden internetin läpi. Sen jälkeen VPN (Virtual Private Network) muodostaa suojatun tunnelin, jonka läpi käyttäjä pystyy käyttämään turvallisesti sisäverkon tiedostoja ja palvelimia.

käyttäjän tietokoneelta reitittimeen luodaan Ciscon AnyConnect-ohjelmalla, minkä jälkeen etäkäyttäjälle avautuu turvallinen pääsy sisäverkkoon.

Kuva 6. Tietomurron kohteena ollut Cisco ASA 5515 VPN-reititin kuvattuna tutkinnan aikana lokakuussa 2024.

ASA 5515 on Ciscon mallistossa suoritusteholtaan ja ominaisuuksiltaan rajoitettu, edullinen laite, joka tukee enintään 250 samanaikaista käyttäjää. Se oli hankittu KASKOa edeltäneen Opetusviraston käyttöön vuonna 2014 mahdollistamaan viraston IT-henkilöstölle pääsy opetuksen sisäverkkoon sekä hyppypalvelimen kautta myös hallintoverkon puolelle. Verkot ovat täysin itsenäisiä, mutta hyppypalvelin on yhteydessä molempiin verkkoihin ja mahdollistaa hallitusti liikenteen verkkojen välillä.

Ciscon ASA 5515 -malli tuli elinkaarensa päähän vuonna 2017, kun sen tuotetuki päättyi. Helmikuussa 2017 valmistaja ilmoitti EOL-aikataulun (End-of-Life), jonka mukaan tilausten vastaanotto loppuisi saman vuoden elokuussa, mutta varaosien saanti huoltosopimuksen tehneille asiakkaille taattiin elokuuhun 2022 asti. Ohjelmiston osalta tuki jatkuu edelleen, sillä sama ohjelmisto toimii myös uudemmissa ASA-sarjan laitteissa. Huhtikuun 2024 lopussa tuorein ohjelmaversio oli 9.12.4, mikä laitteessa olisi pitänyt olla päivitettynä, jos laite olisi haluttu pitää mahdollisimman turvallisena. Ohjelmistojen päivitys edellyttää maksullista tukisopimusta, mutta kriittisten virheiden vaatimat korjaukset Cisco julkaisee kaikille laitteen käyttäjille.

ASA 5515:n tuen päättyminen oli KASKOn tiedossa ja vuoden 2018 lopussa hankittiin VPN-käyttöä varten uudempi ASA 5545 -laite, jolla etäkäyttöyhteydet oli tarkoitus kahdentaa. Laitteen hankinnasta ja ylläpidosta vastannut henkilö lähti kuitenkin KASKOsta keväällä 2020, jolloin 5545 käyttöönotto oli vielä kesken. Palomuurilaite jäi fyysisesti ja valmiiksi konfiguroituna konesalin laiteräkkiin vanhan 5515-laitteen yläpuolelle, mutta sitä ei kytketty verkkoon eikä siinä ollut sähköä.

ASA 5515:n asentamisesta ja arkipäiväisestä ylläpidosta vastasi KASKOn oma IT-henkilökunta. Laitteen tietoturvasta vastanneet avainhenkilöt lopettivat kuitenkin KASKOn palveluksessa 2017, eikä heiltä jäänyt kirjallista dokumentaatiota. Keväällä 2024 ASA 5515 oli yhä käytössä ilman, että kukaan erityisesti valvoi sen toimintaa.

Vuonna 2019 tehtiin hankintaehdotus kahdesta uudesta VPN-laitteesta Ciscon laitteen korvaajaksi. Ehdotus hyväksyttiin KASKOn normaalien käytänteiden mukaisesti, mutta tuntematomasta syystä näitä laitteita ei koskaan tilattu.

Kuva 7. KASKOn konesalin laitekaappi lokakuussa 2024. Kuvassa näkyy VPN-varalaite ASA 5545, jota ei koskaan otettu käyttöön. Tietomurrossa käytetty ASA 5515 sijaitsi sen alapuolella.

VPN-reitittimen siirtoprojekti käynnistyi vuonna 2020, kun KASKOn työntekijöiden käyttäjätunnuksia alettiin siirtää ASA 5515 -laitteesta uuteen, DigiHelsingin ylläpitämään uudempaan VPN-järjestelmään. Siirtoprojekti eteni normaalisti, mutta sitä ei pidetty erityisen kiireellisenä. KASKOn IT-henkilöstöä työllistivät enemmän koulujen tietoliikenneyhteyksien rakentaminen ja verkon aktiivilaitteiden päivittäminen.

Keväällä 2024 ASA 5515 VPN-laitteesta oli siirtämättä vielä 20–30 käyttäjätunnusta. Joillakin käyttäjillä oli tunnus sekä uuteen että vanhaan VPN:ään. Jäljellä olevat ASA 5515:n käyttäjät olivat lähinnä kumppaniyrityksiä, kuten valvontakameroista ja kulunvalvontalaitteista vastanneiden alihankkijoiden työntekijöitä.

Vuoden 2019 aikana Helsingin kaupunki valmisteli Digitaalinen perusta -hanketta, jonka toiminta alkoi vuoden 2021 alusta. Uusi organisaatio rekrytoi KASKOlta kaksi tietoliikenneasiantuntijaa. Tietoliikennepalvelujen tuotantovastuu siirtyi tässä yhteydessä Digitaaliselle perustalle.

KASKOlta siirtyneistä laitteista ei tehty kirjallista listaa, joten ASA 5515:n asema jäi epäselväksi. Digitaalinen perusta (vuoden 2023 alusta yhtiöitetty nimelle DigiHelsinki Oy) katsoi

laitteen kuuluvan edelleen KASKOn vastuulle. Toisaalta ASA 5515:n käytännön ylläpitoa suorittivat myös DigiHelsingin organisaatioon siirtyneet entiset KASKOn työntekijät.

Ylläpitotoimet sisälsivät lähinnä varmenteen päivittämistä sekä käyttäjätunnusten hallintaa. Koska palvelimen osoitteeseen liittyvä edu.hel.fi-varmenne on voimassa vain vuoden kerrallaan, varmennetiedosto piti uusia säännöllisesti. DigiHelsinki tilasi päivitystyön ulkopuoliselta yritykseltä, jonka kanssa sillä oli voimassa oleva sopimus. Viimeisin varmennepäivitys suoritettiin maaliskuussa 2024, koska varmenne oli vanhentumassa 1.4.2024.

Ciscon ASA-laitteissa ohjelmiston ja varmenteen päivitys voidaan tehdä paikallisesti USB-tikulta tai verkon yli etäyhteydellä. Alihankkijana toiminut kaupallinen yritys teki pyydetyt ylläpitotoimet etänä ja testasi muutosten toimivuuden, mutta ei tarkastanut palvelimen ohjelmaversioita eikä toiminta-asetuksia kokonaisuutena.

VPN-käyttäjätunnuksia ASA 5515 -laitteeseen oli luotu vain KASKOn henkilökunnalle sekä ulkoistettujen palvelutarjoajien henkilökunnalle. Oppilailla ei ollut etäkäyttötunnuksia laitteeseen. Käyttäjät todensivat itsensä VPN:lle käyttäjätunnuksella ja salasanalla. Vahvaa tunnistusta, kuten tekstiviestillä lähetettävää kertakäyttöistä salasanaa tai erillistä todennussovellusta ei käytetty, koska sitä ei voitu edellyttää henkilökohtaisten puhelinten käyttäjiltä.

Rehtoreilla, vararehtoreilla, erityisopettajilla ja ammatillisen koulutuksen opettajilla oli käytössä kaupungin hankkima puhelin. Muista opettajista työnantajan puhelin oli vain osalla. Henkilökohtaisen puhelimen käyttäjät eivät halunneet asentaa puhelimeensa erillistä todennussovellusta eivätkä ilmoittaa henkilökohtaista numeroaan työnantajalle, joten vahvaa tunnistautumista ei voitu toteuttaa.

VPN-reitittimen konfiguraatio sisälsi tietomurron kannalta ratkaisevan virheen. Konfiguraatiotiedostossa on tyypillisesti kymmeniä tai jopa satoja muutettavia asetuksia, jotka määritellään graafisen käyttöliittymän avulla tai suoraan tekstitiedostoa muokkaamalla.

Teknisten toiminta-asetusten lisäksi konfiguraatiotiedostossa listataan käyttäjäryhmittäin sisäverkkoon myönnettävät oikeudet. Ellei käyttäjätunnus kuulu mihinkään erikseen määriteltyyn ryhmään, se saa oletusoikeudet (default-group-policy). VPN-palvelimen konfiguraatiotiedostossa oli virheellinen asetus:

```
default-group-policy AC-TUKI
```

Määritys antoi AC-TUKI-ryhmän oikeudet kaikille niille, jotka eivät kuuluneet mihinkään erikseen nimettyyn ryhmään. Ryhmänimi AC-TUKI viittaa AnyConnect-ohjelmaan ja IT-tuen itseään varten luomaan ryhmään, jolle oli toisaalla konfiguraatiossa määritelty vikojen selvittämistä ja korjausta varten laajat pääsyoikeudet kaikkialle sisäverkkoon.

Oikea asetus olisi ollut:

```
default-group-policy DENY
```

Se olisi estänyt pääsyn sisäverkkoon muilta kuin erikseen siihen oikeutetuilta käyttäjiltä. Varalaitteeksi hankitussa 5545-mallissa DENY-asetus oli tehty oikein.

Tutkinnassa ei pystytty selvittämään, miksi tai milloin virheelliset asetukset oli tehty konfiguraatiotiedostoon. Laitteen alkuperäiset asentajat olivat poistuneet Helsingin kaupungin palveluksesta organisaatiouudistuksen yhteydessä vuonna 2017. Konfiguraatiotiedostosta ei löydetty aiempia versioita, joista olisi voitu päätellä lisäyksen ajankohtaa.

Hyökkääjä onnistui kirjautumaan VPN-reitittimelle käyttäen kahden oppilaan tunnusta ja salasanaa. Todennäköisesti tiedot olivat päätyneet pimeään verkkoon aiemman, määrittelemättömän tietovuodon seurauksena.

Oppilastunnuksilla ei ollut oikeuksia palvelimen etäkäyttöön. Tunnukset kuitenkin täsmäsivät opetustoimen vanhaan käyttäjätietokantaan, jonka vuoksi VPN-reititin antoi niille virheellisesti AC-TUKI-ryhmän oikeudet.

Pelkkä tekninen sisäänpääsy ei vielä riitä tiedostojen lukemiseen tai tiedostopalvelinten käyttämiseen. Siksi hyökkääjä alkoi tutkia sisäverkkoa skannaamalla järjestelmällisesti palvelimia ja etsimällä keinoja käyttöoikeuksiensa laajentamiseen. Tavalla, jota tutkinnassa ei pystytty täysin selvittämään, hyökkääjä onnistui kirjautumaan admin-oikeuksilla[23] etätyöpöytäyhteydellä sisäverkon palvelimelle.

Saatuaan jalansijan ensimmäiselle sisäverkon palvelimelle hyökkääjä pystyi murtamaan muita käyttäjätilejä ja näin laajentamaan pääsyään yhä laajemmalle. Hyökkääjän toimintaa helpotti se, että useilla palvelimilla käytettiin samaa salasanaa admin-tunnuksilla. Hyökkääjä sai haltuunsa myös varmuuskopiointipalvelimen admin-tunnuksen, jonka avulla hyökkääjä pystyi lukemaan koko tiedostopalvelimen sisällön.

Yhdeltä palvelimelta hyökkääjä löysi ylläpitohenkilön selaimen sisäiseen varastoon tallentamat salasanat. Niiden joukossa oli sekä henkilökohtaisia salasanoja että KASKOn palvelinten salasanoja.

2.2 Tietomurto verkkolevylle

Windows-tiedostopalvelin (jatkossa ”verkkolevy”) hankittiin Opetusvirastolle arviolta 15–20 vuotta sitten. Laitteen tarkkaa historiaa ei tutkinnassa pystytty selvittämään. Vuosien mittaan käyttäjien määrä lisääntyi ja levytilaa kasvatettiin, joten vanhentuneita tiedostoja ehti kumuloitua mittava määrä.

Tietomurron kohteeksi joutuneelle verkkolevylle oli pääsy kaikilta KASKOn hallinnon työasemilta ja toimipisteiltä. Käyttäjiä oli siten useita tuhansia.

Verkkolevyn käyttöoikeudet oli jaettu oikeaoppisesti organisaatio- ja toimintokohtaisesti, mutta tietomurrossa ne menettivät merkityksensä, sillä hyökkääjän haltuun saamalla varmuuskopiointitunnuksella oli lukuoikeus kaikkiin tiedostoihin.

Verkkolevyn käytössä oli eroja toimipisteiden välillä. Jossain sitä ei käytetty juuri lainkaan, koska käytössä oli pilvipalvelut. Joissain yksiköissä verkkolevyjä käytti koko henkilöstö ja joissain vain hallinnollinen henkilöstö. Erilaiset tarpeet ja vakiintuneet käytännöt olivat synnyttäneet eroja toimipisteiden välille.

Verkkolevy näkyi useimmille käyttäjille tietokoneen V: -levyasemana. Osa kansioista näkyi R: -asemana. Yhteiskäyttöisten asemien lisäksi käyttäjillä oli henkilökohtainen verkkolevy (H: -asema), joka sijaitsi eri palvelinympäristössä. Siihen hyökkääjä ei onnistunut murtautumaan.

Verkkolevyllä valmistellaan, jaetaan ja säilytetään tietoa. Helsingin kaupungilla on useita tietojärjestelmiä, jotka eivät täysin toimi yhteen. Tämän vuoksi tietoja joudutaan tallentamaan ”välivarastoon” verkkolevylle, jotta myös muut käyttäjät pystyvät muokkaamaan niitä.

[23] Admin-oikeudet (administrator) ovat peruskäyttäjän oikeuksia laajemmat ja niillä pystyy tyypillisesti muuttamaan asetuksia sekä ottamaan hallintaan muiden käyttäjien tiedostoja. Admin-oikeudet voivat olla laitekohtaisia tai kattaa laajempia sisäverkon alueita (domain).

Vastaavasti monia päätöksiin liittyviä asiakirjoja valmistellaan ensin verkkolevyllä ja vasta lopulliset tiedot kirjataan aikanaan tietojärjestelmiin.

Verkkolevylle oli vuosikymmenien aikana tallentunut paljon erilaista tietoa (kts. kuva 4). Osa tiedostoista liittyi koulujen toimintaan, kuten ohjeet, tiedotteet ja muistiot. Osa sisälsi luottamuksellisia henkilötietoja, kuten tietoa sairauksista, allergioista tai lääkityksistä.

Verkkolevyn sisältöjä ei vuosien aikana juurikaan arvioitu tai siivottu, eikä sen käytöstä ollut selkeitä ohjeita. Tietojen säilyttämistä verkkolevyllä oli ohjeistettu yleisellä tasolla, mutta ohjeiden noudattamista ei valvottu. Tilapäisiksi tarkoitetut valmisteluasiakirjat jäivät levylle senkin jälkeen, kun niiden käyttö oli päättynyt.

Verkkolevy oli sitä käyttäville yksiköille keskeinen työväline. Tietomurron jälkeen verkkolevy oli pois käytöstä noin kuukauden, mikä aiheutti organisaatioissa runsaasti ylimääräistä työtä. Käyttökatko osui pahimpaan mahdolliseen aikaan, sillä toukokuussa laaditaan todistuksia ja valmistellaan seuraavan lukuvuoden oppilasvalintoja.

Verkkolevy oli toteutettu virtualisoituna palvelimena, joka sijaitsi KASKOn omassa konesalissa. Sen ylläpidosta vastasi KASKOn oma IT-henkilöstö. Levy oli suunniteltu siirrettäväksi DigiHelsingin alaisuuteen niin, että tila olisi ostettu sen alihankkijan konesalista kapasiteettipalveluna. Siirtoa ei kuitenkaan ehditty toteuttaa ennen tietomurron tapahtumista.

Verkkolevyn tiedostomäärä ja niiden käyttö

Tietomurron jälkeen KASKO listasi verkkolevyn varmuuskopiossa olevat tiedostot. Mediaan annetuissa kommenteissa kaupunki kertoi verkkolevyllä olleen ”kymmeniä miljoonia asiakirjoja”.[24]

Tutkintaryhmä analysoi verkkolevyn tiedostolistauksen ja sen havaittiin sisältävän yhteensä 4 983 854 riviä. Kansioita oli 521 774 ja tiedostoja 4 462 080. Ero alkuvaiheessa ilmoitettuun määrään selittyy levyn virustarkistuksella, joka tehtiin varmuuskopioinnin yhteydessä.

Helsingin kaupunki kertoi julkisuuteen virustarkistusohjelman ilmoittaman skannattujen tiedostojen kokonaismäärän. Virustarkistus avaa kaikki löytämänsä tiedostopaketit, kuten ZIP-tiedostot[25] sekä ohjelmien asennuksessa käytettävät CAB- ja MSI-tiedostot[26]. Ohjelmien jakelupaketit eivät sisällä käyttäjän omia tiedostoja, joten ne eivät ole tietomurron kannalta oleellisia. Virustarkistus laskee nämäkin tiedostot mukaan kokonaismäärään.

Käyttöjärjestelmä tallentaa tiedostoista vähintään kaksi aikaleimaa: tiedoston perustamishetken sekä viimeisen ajankohdan, jolloin tiedosto on muokkauksen jälkeen tallennettu. Joissakin tapauksissa tallentuu myös viimeinen käyttöhetki, joka voi liittyä tiedoston avaamiseen lukemista varten tai esimerkiksi ohjelmatiedoston käynnistämiseen. Windowsin tavallinen tiedostolistaus näyttää tiedostoista vain viimeisen tallennusajankohdan.

Koska tiedostoja oli vuosien mittaan kerätty levylle eri lähteistä, aikaleimat eivät kaikissa tapauksissa ole täysin luotettavia. Leimoista voi kuitenkin päätellä, että levylle luotiin eniten uusia tiedostoja vuosina 2020 ja 2021, minkä jälkeen vuosittaiset uusien tiedostojen määrät putosivat noin puoleen.

---

[24] Yle-uutinen 25.5.2024: Helsingin kaupungin selvitys paljastaa yhä vakavampia piirteitä tietomurrosta. 26.2.2025 https://yle.fi/a/74-20090447

[25] ZIP on yleisesti käytetty häviötön pakkaustekniikka, jolla tiedostoja kootaan yhteen ja tiivistetään niin, että ne vievät vähemmän tilaa levyllä.

[26] CAB (Cabinet) ja MSI (Microsoft Installer) ovat Windows-sovellusten asennuspaketteja, joissa on kaikki ohjelman tarvitsemat tiedostot ja alkuperän varmistava ohjelman tekijän digitaalinen allekirjoitus.

Muutospäiväysten perusteella tiedostoja muokattiin eniten vuonna 2019, minkä jälkeen myös muokattujen tiedostojen määrä laski tasaisesti vuosittain.

Verkkolevylle tallennetuista asiakirjoista keskeisiä ovat Microsoft Officella tehdyt Word-, Excel- ja PowerPoint- sekä PDF-tiedostot.

Tutkinnassa tarkasteltiin listauksen tiedostonimiä. Niiden perusteella Office-asiakirjoissa oli mm. pöytäkirjoja, sisäilmatutkimuksia, remontteihin liittyviä suunnittelukokouspöytäkirjoja, kauppakuitteja, pohja- ja rakennuspiirroksia, käsikirjoja, ohjeita, rikosilmoituksia, suunnitelmia, toimintakertomuksia ja -suunnitelmia sekä esityslistoja.

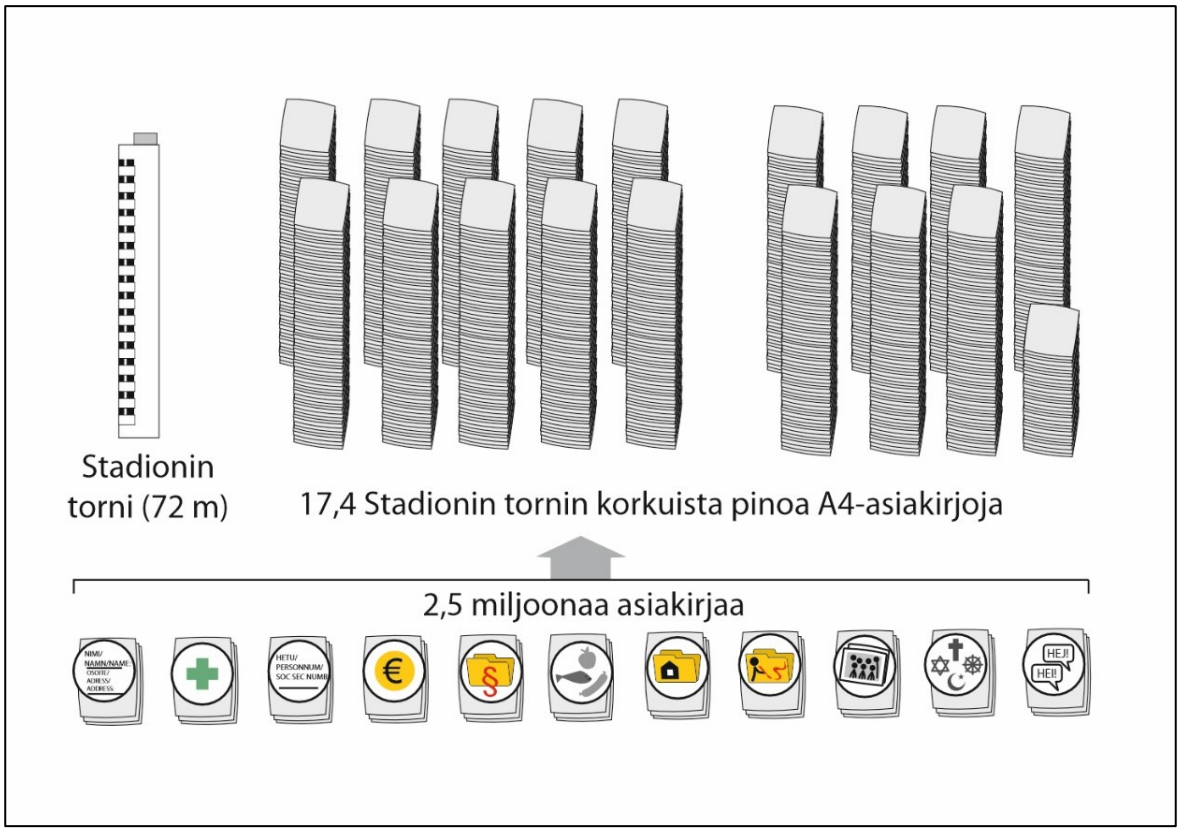
Taulukko 1: Asiakirjatyypit ja niiden kappalemäärät

Asiakirjan tyyppi	Kappalemäärä
Word (DOC, DOCX)	1 094 684
Excel (XLS, XLSX)	513 060
PowerPoint (PPT, PPTX)	109 378
PDF-tiedostot (PDF)	766 455
Yhteensä	**2 483 577**

PDF-tiedostoissa voi olla paitsi alkuperäisiä asiakirjoja, myös skannerilla luettuja paperidokumentteja. Nimistä päätellen tiedostoissa oli mm. ajokortteja, hygieniapasseja, laskuja, tilauksia, lääkärintodistuksia, avustajahakemuksia, tiedotteita, henkilökohtaisia palkkiolaskelmia, virkavapauspäätöksiä, oppilasarviointeja, verokortteja, viranhoitomääräyksiä, eroilmoituksia, tapaturmailmoituksia vakuutusyhtiölle sekä palkkalaskelmia.

Asiakirjojen luonteen vuoksi lähes kaikissa on oletettavasti henkilöihin yhdistyviä ja heitä yksilöiviä henkilötietoja. Erityisen luottamuksellisia asiakirjoja olivat erityisen tuen päätökset, päiväkotimaksuihin liittyvät selvitysaineistot, lääkärintodistukset, passikopiot sekä vanhempien henkilö- ja tulotiedot.

Tiedon määrää voidaan havainnollistaa oletuksella, että jokaisessa asiakirjassa on viisi tulostettavaa sivua. Silloin asiakirjoissa olisi yhteensä 12,5 miljoonaa tulostettavaa sivua ja koska yhden A4-arkin paksuus on noin 0,1 millimeriä, yksipuoleisina A4-paperitulosteina ne muodostaisivat 1,25 km korkean pinon.



Kuva 8. Havainnekuva verkkolevylle tallennettujen asiakirjojen määrästä.

Kansionimistä päätellen verkkolevyllä oli runsaasti myös muilta levyiltä siirrettyjä tiedostoja sekä USB-tikuilta tehtyjä varmuuskopioita. Varsinaisten asiakirjojen lisäksi levyllä oli yli 1,1 miljoonaa JPEG-valokuvaa mm. päiväkotien ja koulujen retkiltä sekä erilaisista tapahtumista. Muita verkkolevyltä tunnistettuja tiedostotyyppejä olivat videotiedostot, sähköpostit (MSG), web-sivut (HTM), animoidut kuvat (GIF), tavalliset tekstitiedostot (TXT) sekä ohjelmistojen asennuspaketit.

Vuotaneiden tiedostojen määristä voidaan puutteellisten lokien vuoksi saada vain summittainen kuva. Tiedostot siirrettiin hyökkääjän palvelimelle FileZilla FTP-ohjelman[27] suojatulla yhteydellä. Liikenteen kokonaismäärä voitiin selvittää palomuurilokeista, mutta salauksen vuoksi tiedostonimiä tai muita yksityiskohtia ei pystytty selvittämään.

Hyökkääjä asensi FileZillan useille palvelimille, mutta poisti ohjelmat käytön jälkeen, joten ohjelman omista lokeista ei ollut apua selvitystyössä. Yhden palvelimen RAM-muistista pystyttiin lukemaan jälkiä siirretyistä tiedostonimistä ja verkkolevyn kansioista, mutta lista oli epätäydellinen. On siten mahdotonta selvittää varmaksi, mitä yksittäisiä tiedostoja tai kansioita hyökkääjä sai haltuunsa.

Hyökkääjän ulos siirtämän datan kokonaismäärästä (kaksi teratavua) suhteesta verkkolevyn tiedostojen kokonaismäärään (6,73 teratavua) voidaan arvioida, että 30 % tiedostoista ehdittiin kopioida, ts. hyökkääjän haltuun päätyi noin 1,3 miljoonaa tiedostoa, joista asiakirjoja (Office ja PDF-tiedostot) oli noin 750 000 kappaletta.

[27] FTP (File Transfer Protocol) on vanha tiedostojen siirtoon kehitetty menetelmä. Alkuperäinen FTP siirtää tiedostot ilman salausta, mutta FileZilla käyttämä uudempi SFTP-menetelmä (Secure FTP) sisältää myös salauksen.

2.3 Tietomurto käyttäjätietokantaan

Verkkolevyn tiedostojen lisäksi hyökkääjä sai haltuunsa myös koko kaupungin hallinnon AD:n käyttäjätiedot sekä perusopetuksen ja ammatillisen opetuksen AD-tietokannat. AD (Active Directory) on Microsoft-verkon keskitetty käyttäjähakemisto, joka sisältää käyttäjätunnukset, sähköpostiosoitteet ja niihin liittyvät henkilötiedot sekä KASKOn tapauksessa myös oppilasnumerot.

2.4 Kyky havainnoida verkkoympäristöä

KASKOn sisäverkon työasemissa oli käytössä haittaohjelmien torjuntaohjelma. Lisäksi palvelimille oli asennettu tietoturvaohjelmisto huolehtimaan palvelimen turvallisuudesta. KASKOlla ei kuitenkaan ollut kattavaa verkkoliikenteen analysointiin ja sen poikkeamien (anomaliat) havainnointiin kykenevää seurantaa.

KASKOn ja DigiHelsingin palomuuripalveluita valvova alihankkija kerää tietoa kaupungin sisäisen ja internet-verkon välisestä liikenteestä. Näiden lokien avulla on voitu jälkikäteen selvittää tietomurron valmisteluun ja itse hyökkäykseen liittyviä tapahtumia helmi-toukokuulta 2024. Palomuuripalveluun ei kuulunut reaaliaikaista hälytysten valvontaa.

Hyökkääjän käyttämä living off the land -tekniikka vaikeutti toiminnan havaitsemista, koska aktiivinen hyökkäys voidaan tunnistaa lähinnä vain verkon ja ohjelmien poikkeavasta käyttäytymisestä.

Hyökkääjän näkökulmasta menetelmän heikkoutena on pysyvän jalansijan puuttuminen. Jos rikollinen toiminta havaitaan, yhteyden katkaiseminen, salasanojen vaihtaminen ja haavoittuvuuksien korjaaminen riittää hyökkääjän karkottamiseen.

Helsingin kaupunki pyrki parantamaan verkkoympäristön valvontaa ja käynnisti kyberturvallisuuden palvelujärjestelmän (Cyber Security Operations Center, CSOC) hankinnan 28.6.2021 julkaistulla EU-hankintailmoituksella. Hankintailmoituksen mukaan CSOC hankitaan Helsingin kaupungin omistamien ja hallinnoimien sekä kolmannelta osapuolelta hankittujen tai vuokrattujen ICT-järjestelmien ja palveluiden kyberturvallisuuden ylläpitämiseksi.

Tarjouspyyntöön saatiin vastaus yhdeltä toimittajalta. Kansliapäällikkö teki asiasta hankintapäätöksen 28.10.2021 niin, että valintaperusteena oli kokonaistaloudellinen edullisuus eli hinta. Hankittaville palveluille oli asetettu vähimmäisvaatimuksina laadullisia vaatimuksia (laatukriteereitä), jotka tarjottavien palveluiden tuli täyttää. Hankinnan ennakoitu arvo oli neljän vuoden mukaan laskettuna 5,2 miljoonaa euroa. Hankintasopimus allekirjoitettiin 4.4.2022.

Hankintapäätöksen jälkeen toimittaja ja kaupunki aloittivat käyttöönottoprojektin. Palvelusopimuksen mukaisesti käyttöönottoprojektin lopuksi toteutettiin palvelun testaus. Kaupunki hankki testausta varten ulkopuolisen toimijan, joka suoritti työn 11.5.-31.5.2023. Kokonaisuus ei läpäissyt hyväksymistestausta. DigiHelsinki teki toimittajalle irtisanomisilmoituksen 16.6.2023 ja käyttöönottoprojekti keskeytettiin.

2.5 Olosuhteet

Kyberturvallisuuskeskus[28] ja Suojelupoliisi[29] järjestivät huhtikuussa 2023 yhteisen tiedotustilaisuuden[30], jossa kerrottiin, että Suomen kyberuhkataso on pysynyt kohonneena, ja että ensimmäisen kerran kyberuhkatasoa nostettiin virastojen yhteistyössä syksyllä 2022.

Kyberturvallisuuskeskuksen saamien ilmoitusten mukaan suomalaisiin organisaatioihin kohdistuvissa kyberhyökkäyksissä erityisesti haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten lukumäärät olivat kasvaneet. Kyberturvallisuuskeskuksen analyysin mukaan suomalaisiin organisaatioihin kohdistuvat hyökkäykset vaikuttivat aiempaa räätälöidymmiltä ja tarkemmin kohdistetuilta. Kybervakoilun ja kybervaikuttamisen yritysten osalta Suojelupoliisi vahvistaa Kyberturvallisuuskeskuksen arvion.

Keskeinen uhkatasoa nostava tekijä on ollut sekä organisaatioita että kansalaisia vastaan kohdistetun verkkorikollisuuden yleistyminen. Myös valtiolliset toimijat ovat aktivoituneet digitaalisessa toimintaympäristössä. Oleellinen muutos organisaatioihin kohdistuvissa tietoturvauhkissa on 2020-luvulla ollut lunnas- eli kiristyshaittaohjelmilla tehtyjen hyökkäysten yleistyminen. Tätä ilmiötä on käsitelty Kyberturvallisuuskeskuksen Tietoturva nyt! -teemaan liittyvässä ”Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa” ajankohtaiskatsauksessa syyskuussa 2024.[31]

Kyberturvallisuuskeskus tiedotti 7.3.2024 eli alle kaksi kuukautta ennen tietomurron tapahtumista Tietoturva Nyt! -artikkelissaan "Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena"[32] verkon reunalaitteisiin liittyvistä riskeistä ja kuinka ne avaavat oven organisaation tietotekniseen ympäristöön.

Kyberturvallisuuskeskuksen kuukausittain julkaistava Kybersää[33] kertoo merkittävistä tietoturvapoikkeamista ja -ilmiöistä Suomessa. Toukokuun 2024 kybersäätila julkaistiin 13.6.2024. Tiedotteen ingressissä todetaan kybersään jatkuneen pilvisenä myös toukokuussa. Tilannetta synkensivät erityisesti tietoon tulleet tietomurrot ja -vuodot. Kybersään yhteenvetotaulukossa nostetaan esille Helsingin kaupungin tapaus toteamalla, että Helsingin kaupungin kasvatuksen ja koulutuksen toimialaan kohdistui laaja tietomurto. Tietomurtojen osalta toukokuun tilannetta kuvattiin vakavaksi, mikä on asteikon kriittisin arvio.

Suurimmassa osassa tietomurtoja tekijöiden tavoitteena on taloudellinen hyöty. Jossain tapauksissa syynä voi olla omien kykyjen testaaminen tai esitteleminen, kaupallisesti arvokkaan tiedon varastaminen kilpailijalta tai yhteiskunnallinen vaikuttaminen.

---

[28] Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt. 25.2.2025 https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

[29] Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt. 25.2.2025 https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

[30] Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut. 25.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara

[31] Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa. 26.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa

[32] Tietoturva Nyt! -artikkeli "Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena” https://www.kyberturvallisuuskeskus.fi/fi/ajankoh-taista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena

[33] Kybersää 26.2.2025 www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

2.6 Lokitiedot

KASKOn verkkolaitteiden, palvelimien ja päätelaitteiden lokienhallinta pohjautui pääasiassa laitteiden sisäiseen lokitukseen, eikä siinä ollut yhdenmukaisia käytäntöjä tai keskitettyä hallintaa. Siksi tietomurtotutkintaa jouduttiin tekemään osin puutteellisin tiedoin. Keskeiseksi tietolähteeksi nousivat DigiHelsingin alihankkijan ylläpitämän palomuurin tiedot, jotka liittyvät lähinnä liikenteeseen internetin ja KASKOn sisäverkon välillä. Sisäverkon palvelimien ja päätelaitteiden tapahtumista oli käytettävissä vain niukasti tietoja.

KASKOn palvelutarjoajilla oli joitakin palvelin- ja verkkotason valvontapalveluita, jotka tuottivat hälytyksiä KASKOn palvelinympäristössä tapahtuneista hyökkääjän toimenpiteistä, jotka tunnistettiin tietomurron selvitystyön aikana. Hälytyksiä ei valvottu siten, että ne olisivat aiheuttaneet torjuntatoimia tietomurron ollessa käynnissä.

2.7 Helsingin kaupunki

Helsingin kaupunki on Suomen suurin työnantaja, jonka palveluksessa oli vuoden 2023 lopussa noin 37 000 työntekijää. Organisaatio jakautuu neljään päätoimialaan: Kasvatus ja koulutus (KASKO), Kaupunkiympäristö (KYMP), Kulttuuri ja vapaa-aika (KUVA), sosiaali-, terveys- ja pelastustoimi (SOTEPE). Lisäksi Helsingin kaupungilla on keskushallinto (kaupungin kanslia). Tietomurron kohteeksi joutunut Kasvatuksen ja koulutuksen toimiala on näistä suurin ja sen palveluksessa on noin 15 000 henkeä. Helsinki on organisoitu suomalaisista kaupungeista poikkeavasti, sillä toimialat ovat hyvin itsenäisiä ja kanslialla on tilaajamainen tai valvova rooli suhteessa toimialoihin.

Kasvatuksen ja koulutuksen toimiala vastaa varhaiskasvatuksesta, esiopetuksesta, perusopetuksesta, lukio-opetuksesta, suomenkielisestä ammatillisesta koulutuksesta ja vapaasta sivistystyöstä. Toiminta on hyvin laajaa; esimerkiksi peruskouluja on noin sata ja niissä opiskelee noin 45 000 lasta ja nuorta. Päiväkoteja on noin 320 ja niissä annetaan varhaiskasvatusta noin 27 000 lapselle.

KASKOlla on oma hallinto- ja tukipalveluorganisaatio, johon sisältyy noin 80 hengen tietohallinto. Näistä noin 20 henkeä toimii ICT-infran ja sen tietohallinnon parissa. Kokonaisuutena tietohallinto on toiminut hyvin itsenäisenä ja erillisenä muiden kaupungin toimialojen tietohallinnosta.

Helsingin kaupunki vahvisti tietoturvalinjaukset 1.6.2020. Tietoturvalinjauksissa esitettiin kaupunkiorganisaatiota sitovat periaateluontoiset ratkaisut tietoturvallisuuden edistämiseksi ja varmistamiseksi. Asiakirjassa on esitetty 14 erilaista linjausta, ja ne sisältävät muun muassa vastuunjaon perusteet.

Kaupungin tiedonhallinnan kokonaisohjaus ja koordinointi toteutetaan tiedonhallintaryhmässä, jonka kaupunginhallitus on asettanut 21.3.2022. Tiedonhallintaryhmän tehtävänä on koordinoida kaupunkitasoisesti tiedonhallintaan liittyvien velvoitteiden edellyttämiä toimenpiteitä, ohjeistusta sekä viestintää ja koulutusta. Tiedonhallintaryhmä kehittää, seuraa, valvoo ja raportoi tiedonhallintaan liittyvien velvoitteiden toteutumista Helsingin kaupungin organisaatiossa. Tiedonhallintatyöryhmän työskentely on ollut säännöllistä, hyvin resursoitua ja sen toimintaan on osallistuttu aktiivisesti. Tiedonhallintatyöryhmän toiminta on pystynyt edistämään kaupungin tiedonhallintavelvoitteiden täytäntöönpanoa ja tietoturvallisuuden kehittämistä. Samana keväänä KASKOssa perustettiin oma tiedonhallinnan koordinaatioryhmä, jonka

tehtävänä on koordinoida toimialatasoisesti tiedonhallintaan liittyvien velvoitteiden edellyttämiä toimenpiteitä, ohjeistusta sekä viestintää ja koulutusta. Ryhmän tehtävänä on lisäksi seurata, valvoa ja raportoida tiedonhallintaan liittyvien velvoitteiden toteutumista toimialalla.

Kaupungin tiedonhallintaryhmässä laaditaan vuosittain tiedonhallinnan valvontasuunnitelma ja käsitellään toimialojen, liikelaitosten ja virastojen antamat tilannekatsaukset. Valvontasuunnitelmalla kaupunki huolehtii sille kuuluvasta lakisääteisestä tietojen käsittelyn ohjaus- ja valvontavelvollisuudesta.

Omavalvonnan tavoitteena on kehittää kaupunkitasoista tiedonhallintaa, huomioida muutokset toimintatavoissa ja tietojärjestelmissä sekä raportoida kansliapäällikölle. Raportit antavat kattavan kuvan tiedonhallintaryhmän toiminnasta ja havainnoista. Raporteissa on tunnistettu myös tiedonhallintaympäristöön liittyviä riskejä, kuten tietojärjestelmien suuri määrä ja hajanaisuus sekä puutteelliset tiedonhallintaympäristöt.

Helsingin kaupungin sisäisen tarkastuksen helmikuussa 2023 valmistuneessa tarkastusraportissa on tunnistettu, ettei vastuunjako tietoturvassa kaupungin kanslian ja toimialojen (ml. KASKO) välillä ollut selvää. Tähän annettiin suositus, jonka mukaan KASKOn tuli päivittää omaa vastuunjakotaulukkoaan syyskuun 2023 loppuun mennessä. Osana tarkastusta tehtiin kysely ja siinä KASKO oli neljästä tarkastellusta toimialasta kaikkein tyytyväisin oman tietoturvansa tasoon.

Raportissa tunnistettiin myös, ettei Helsingin kaupungilla ole tehokkaita keinoja havaita verkkohyökkäyksiä. Osaltaan syynä olivat viiveet tähän liittyvän palvelun hankinnassa ja käyttöönotossa. Asiaan annettiin suositus hankkia keskitetty valvontapalvelu toukokuun 2023 loppuun mennessä. Kilpailutuksen epäonnistumisen vuoksi palvelua ei saatu hankittua toukokuuhun 2024 mennessä, eikä se siten ollut käytössä tietomurron tapahtuessa.

Viranhaltijoiden vastuut

Helsingin kaupunginhallitus on 28.2.2022 tekemällään päätöksellä vahvistanut Helsingin kaupungin tiedonhallinnan ja asiakirjahallinnon ohjeistuksen, käytännöt, vastuut ja valvontamekanismit. Päätöksen mukaan vastuu tiedonhallintaan liittyvien toimenpiteiden toteutuksesta on toimialojen, virastojen ja liikelaitosten johtavilla viranhaltijoilla. Johtavat viranhaltijat määrittelevät toteutusvastuulliset tahot omassa organisaatiossaan.

Kaupunkitasoiset vastuut on määrätty mainitussa kaupunginhallituksen päätöspöytäkirjassa. Digitalisaatiojohtaja vastaa tiedonhallintamalliin tietohallintoon liittyvästä kaupunkitason ohjauksesta. Erityisesti digitalisaatiojohtaja vastaa tiedonhallintalain[34] 5 §:n mukaisen tietojärjestelmien, -varantojen sekä integraatioiden ja rajapintojen nykytilan kuvauksen ja muutosvaikutusten suunnittelun, ohjeistuksen ja toimeenpanon seurannan organisoimisesta kaupunkitasolla.

Tiedonhallintapäällikkö huolehtii kaupungin asiakirjahallinnon johtamisesta, antaa ohjeita asiakirjahallinnon vastuista, tehtävistä ja käytännöistä, ohjaa ja kehittää kaupungin asiakirjahallintoa osana tiedonhallintaa, hyväksyy kaupungin yhteisen tiedonohjaussuunnitelman, valvoo ohjeiden noudattamista sekä huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta (sisältää tietoturvan ohjausvastuun analogisen aineiston arkistokelpoisuudesta, arkistotiloista ja asiakirjojen suojaamisesta poikkeusoloissa).[35]

[34] 906/2019.
[35] Helsingin kaupunginhallituksen delegointipäätös (24.4.2017 § 441).

KASKOssa aihealueen kehittämistehtävät oli organisoitu kaupunkiorganisaation yhteisiä kehittämistyöryhmiä vastaavalla tavalla. Kehittämistehtäviä varten oli koottu neljä erillistä työryhmää ja niihin oli nimetty asiantuntijoita toimialalta. Tällä pyrittiin varmistamaan, että tiedonhallintalain ja tietosuoja-asetuksen muuttuneet velvoitteet saadaan toteutettua. Työryhmien työskentelyn yhteydessä havaittiin kuitenkin, että työryhmiä on liikaa ja niiden toiminta keskenään heikosti koordinoitua. Myöhemmin näistä syistä työryhmäjärjestelyjä uudistettiin.

KASKOn toimialajohtaja teki 28.5.2020 päätöksen alaistensa viranhaltijoiden tiedonhallintavastuista. Päätöksellä tietosuojaan, tietoturvallisuuteen, tiedonhallintaan ja tietoteknisiin ratkaisuihin liittyviä tehtäviä jaettiin toimialan viranhaltijoille. Tehtävät kuvattiin luonnehtimalla niiden sisältöjä lyhyin lausein tai asiasanoin. Keskeisiä viranhaltijoita olivat hallintojohtaja, tietojärjestelmäpäällikkö ja tietohallintopäällikkö, sekä yksikön päällikkönä toimiva työsuhteinen tietoturvapäällikkö.

Ohjeistusta tiedonhallintaan, tietosuojaan ja tietoturvaan Helsingin kaupungilla on laajasti. Ohjeista osa on kaupungin yhteisiä ja osa toimialojen sisäisiä. Kaupunginkansliaan sijoitettu tiedonhallintayksikkö on ylläpitänyt 33 erillistä tiedonhallintaa ja tiedonhallintatapaa koskevaa ohjetta.

Tiedonhallinnan ohjausryhmä valmisteli 27.9.2022 oppaan tiedonhallinnan virkavastuista. Opas suunnattiin yleisesityksenä kaupungin esihenkilöstölle. Asiakirjassa esitettiin tiedonhallinnan toteuttamisen rakenteet. Oppaassa todetaan muun muassa, että kaupungin on pidettävä käsittelemistään asioista asiarekisteriä. Siihen kuuluvat asiat, joissa tehdään jonkinlainen ratkaisu. Asioiden valmistelijoiden on huolehdittava, että asioiden käsittelyvaiheet asiakirjoineen rekisteröidään viipymättä, jotta rekisteri pysyy ajan tasalla. Oppaan mukaan kaikki asiakirjat eivät kuulu asiarekisteriin vaan niitä koskevat tiedonhallintalain 27 §:n palvelujen tiedonhallinnan määräykset. Työtehtäviin liittyvät asiakirjat tulee rekisteröidä ja hallita niin, että ne löytyvät vaivatta, vaikka niistä ei ole tehty hallinnollista päätöstä.

Ohjeessa todetaan myös, että tiedonhallintamallissa on oltava merkintä, josta käy ilmi tietovarantojen tietoaineistojen säilytysmuoto, -tapa ja -aika sekä tieto siitä, miten aineistot hävitetään, mikäli näin on määritelty laissa tai tiedonohjaussuunnitelmassa. Pysyvästi säilytettävät tiedot on säilytettävä asianmukaisesti ja tuhottavaksi määritellyt tiedot on hävitettävä säilytysajan umpeuduttava. Järjestelmät, joissa asiakirjoja tuotetaan asiarekisteriin, on kuvattava asiakirjajulkisuuskuvauksessa.

Kaupunginkanslian 14.3.2022 päivätyssä ohjeessa ”Väliaikainen ohje tietoaineistojen sähköisestä säilyttämisestä” linjataan, että asiakirjojen valmistelu ja säilytys tulee toteuttaa keskitetyssä hallintajärjestelmässä (Ahjo). Ohje kuitenkin sallii mm. seuraavan poikkeuksen:

> ”*Kaupungilla ei ole vielä tarjota digitaalisia työvälineitä kaikkien tehtävien hoitoon, joten työtä tehdään myös analogisesti eli käytetään paperisia asiakirjoja. Asianhallinta- ja dokumentinhallintaratkaisujen hankintaa valmistellaan. Kaupunkiyhteisten asiakirjojen säilytysratkaisujen puuttuessa sähköinen säilyttäminen täytyy ratkaista väliaikaisesti, koska velvoite on tullut voimaan 1.1.2022. Asiakirjat, joiden säilyttämiseen ei ole soveltuvaa sähköistä tietojärjestelmää, tallennetaan verkkolevylle yhteiskäyttöiseen kansioon*.”

Tiedonhallintamalli, joka ohjaa Helsingin kaupungin toimintaa, muodostuu useista eri kokonaisuuksista. Siihen sisältyvät tietovarantojen ja tietojärjestelmien kuvailut (arkkitehtuurikuvat), sovellusluetteloita, prosessikuvauksia, tiedonohjaussuunnitelmia ja

riskienarviointiaineistoa. Lisäksi tiedonhallintamalliin voidaan katsoa kuuluvaksi vastuuhenkilö- ja periaatepäätökset.

KASKOn tietojärjestelmän arkkitehtuurikuvauksessa on esitetty toimialalla käytettävät tietojärjestelmät, tietovarannot ja tietojen hallinnan yleisperiaatteet. Kuvauksista puuttuu tietomurron kohteeksi joutunut verkkolevy.

Tiedonohjaussuunnitelmaa Helsingin kaupunki ylläpitää osana tiedonohjausjärjestelmäänsä.[36] Järjestelmän on tarkoitus sisältää kaikki Helsingin kaupungin tiedonohjaustiedot tiedon muodosta riippumatta (sähköiset aineistot ja paperiaineistot).

Tiedonohjaussuunnitelma valmistui vuonna 2019 kaikille tehtäväluokille. Tiedonohjaussuunnitelma on luonteeltaan jatkuvasti päivittyvä ja ajantasainen versio on saatavilla tietoverkossa.

Työntekijöiden keskuudessa KASKOn tiedonhallinnan prosessit on koettu monimutkaisiksi. Esimerkiksi sähköisesti allekirjoitettu lomake saatetaan joutua tulostamaan, allekirjoittamaan käsin ja sitten skannaamaan järjestelmään. Joissakin kouluissa vain rehtori ja koulusihteeri käyttävät verkkolevyä. Opettajat käyttävät lisäksi muita ratkaisuja, esimerkiksi käytössä olleita pilvipalveluratkaisuja ja oman tietokoneen tallennustiloja. Koulujen ja henkilöiden välillä on eroa siinä, mitä menettelyjä tiedon tallennukseen käytetään.

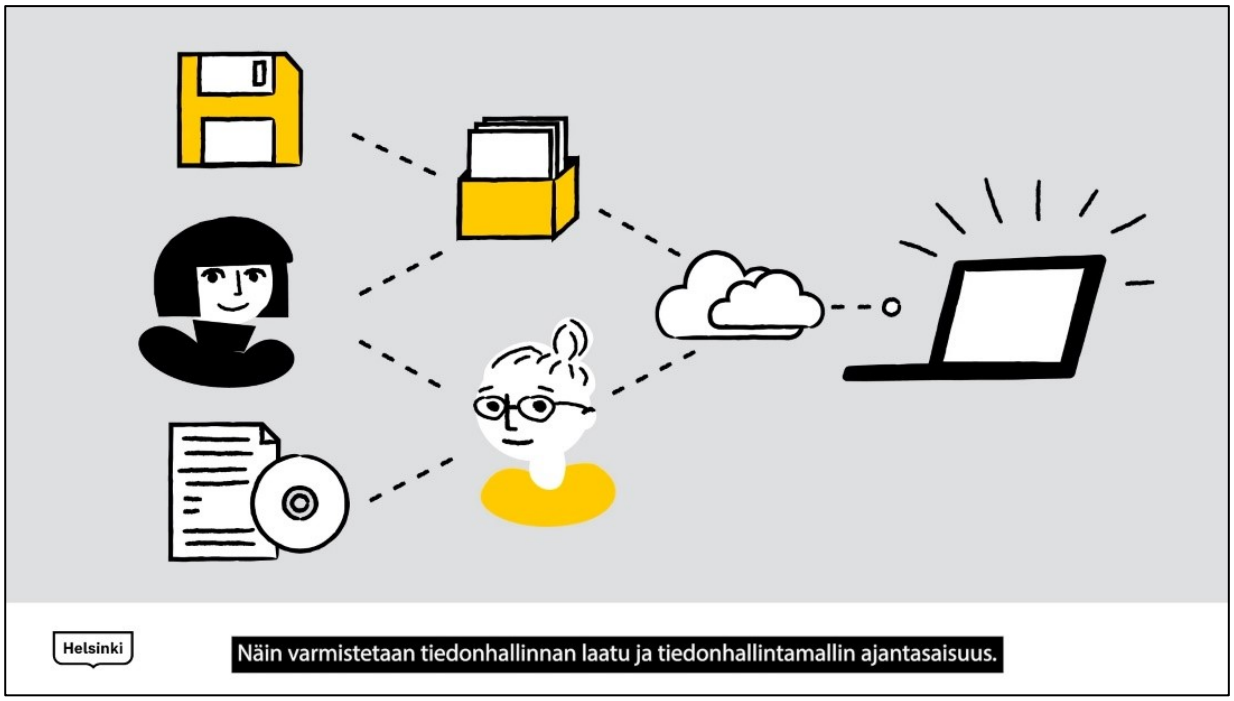
Työntekijöiden DigiABC-koulutus

Helsingin kaupunki on tehnyt tietosuojasta ja -turvallisuudesta DigiABC-videokoulutuksen. Noin tunnin pituisen koulutuksen pystyy suorittamaan itseopiskeluna omalta tietokoneelta ja se sisältää lopuksi monivalintatentin. Kaupunginkanslia on tuottanut tietoturvan opetusvideoita myös internetiin avoimesti katsottaviksi.

Lähtökohtaisesti uuden työntekijän tulee suorittaa DigiABC kahden viikon kuluessa, mutta suoritusmäärät vaihtelevat toimialakohtaisesti. Koulutusvideoiden sisältöä päivitetään säännöllisesti, joten pidempään talossa olleiden pitää uusia koe. Esihenkilöt seuraavat suoritettujen koulutusten määrää. Lisäksi kaupunki on tarjonnut tiedon- ja asiakirjahallinnan peruskursseja.

Keväällä 2024 DigiABC-koulutus käsitteli yleisten tietoturva-asioiden lisäksi myös tietojen luokittelua ja suojausmerkintöjä. Tietosuojasta opastettiin yleisellä tasolla henkilötietojen merkitykseen ja turvalliseen käsittelyyn. Tiedon elinkaarta ja vanhentuneiden tietojen poistamista ei erikseen mainittu.

[36] Helsingin Kaupunki: Tiedonohjausjärjestelmä. 26.2.2025. https://tiedonohjaus.hel.fi



Kuva 9. Ruutukuva Helsingin kaupungin DigiABC-itseopiskelukoulutuksesta.

DigiHelsinki Oy on Helsingin kaupunkikonserniin kuuluva osakeyhtiö, joka on rekisteröity kaupparekisteriin 2.8.2022. Vuonna 2023 sen liikevaihto oli noin 58 miljoonaa euroa ja se työllisti 134 henkilöä. Helsingin kaupunki omistaa yhtiön osakkeista 100 prosenttia sekä käyttää hankintalain edellyttämällä tavalla ratkaisevaa vaikutusvaltaa yhtiön strategisiin tavoitteisiin ja tärkeisiin päätöksiin hallituksen jäsenten nimeämisoikeuden, omistajaohjauksen ja konsernivalvonnan keinoin.

Yhtiön tehtävänä on tuottaa digitaalisia peruspalveluita Helsingin kaupungille. Tällaisia palveluita ovat muun muassa ensimmäisen asteen tuki, luottamushenkilöorganisaatioiden kokousten tukipalvelu, lähitukipalvelu, päätelaitteiden elinkaaripalvelut, vakio-ohjelmistopalvelut, tulostuspalvelut, lähiverkko, tietoliikenneliittymät, palomuuri, runkoverkko, palvelin ja tallennusjärjestelmien kapasiteettipalvelut, tietokantapalvelut, varmistus ja palautus, AD-hakemisto, työryhmäpalvelut, IT-asiantuntijapalvelut, kyberturvapalvelu, asiakastyöasemien tukipalvelut sekä infonäyttöpalvelu.[37]

Yhtiön perustamisen taustalla on vuonna 2019 aloitettu Digitaalinen perusta -hanke, jonka tarkoituksena oli käynnistää toimet kaupungin digitaalisen toimintaympäristön päivittämiseksi ja modernisoimiseksi. Digitaalinen perusta -hanke sisältyi Helsingin kaupungin laajempaan digitalisaatio-ohjelmaan vuosille 2019–2022 ja oli ohjelman keskeinen kehittämiskohde. Hanke organisoitiin osaksi kaupunginkanslian strategisen osaston toimintaa ja osa kaupungin IT-henkilöstöstä siirtyi kaupunginkansliaan perustettuun toimintayksikköön. Tässä muodossa toimintaa jatkettiin vuoden 2023 alkuun saakka, jolloin toiminnot siirrettiin niiden tuottamista varten perustettuun DigiHelsinki Oy:hyn. Yhtiöittämisen myötä lisää kaupungin IT-henkilöitä siirtyi DigiHelsingin palvelukseen.

Yhtiöittämispäätöksen mukaisesti DigiHelsinki Oy toimii kaupungin ja sen tytäryhteisöjen yhteishankintayksikkönä, mikä on kirjattu yhtiön toimialaksi sen yhtiöjärjestykseen. Yhteishan-

[37] Kaupunginvaltuusto §142 1.6.2022

kintayksikkönä yhtiö voi kilpailuttaa kaupungin ja sen tytäryhteisöjen käyttöön mm. puitejärjestelyitä ja dynaamisia hankintajärjestelmiä, joiden kautta kaupunki ja tytäryhteisöt voivat hankkia tavaroita tai palveluja. Tietoliikennelaitteiden asennuspalvelun toimittajaksi valittiin kilpailutuksella Dustin Finland Oy.

DigiHelsinki Oy tuottaa digitaalisia peruspalveluja kaupunkitasoisen puitesopimuksen sekä käyttäjäorganisaatiokohtaisten (esim. toimiala, virasto ja liikelaitos) liityntäsopimusten ja vuosittaisten käyttäjäorganisaatiokohtaisen hankintapäätöksen mukaisesti. Poikkeamista kaupunkitasoisiin palveluihin on määrätty sovittavaksi käyttäjäorganisaatiokohtaisissa liityntäsopimuksissa. Kaikki kaupungin toimialat ovat tehneet 1.1.2023 alkaen voimassa olleet hankintasopimukset yhtiön kanssa. Sopimuksen mukaisissa toimituksissa ja palveluiden laajuuksissa on toimialuekohtaisia eroavaisuuksia. ICT-palvelukokonaisuuksien siirtäminen kerralla uudelle yhtiölle koettiin haastavaksi, joten palvelujen siirtoa vaiheistettiin muun muassa siten, että KASKOlle jäi edelleen omaa ICT-peruspalvelutuotantoa ja ICT-henkilöstöä.

Yhtiön toiminnan alkamisen ja toimialakohtaisten hankintasopimusten tekemisen jälkeen on edelleen jatkunut tilanne, jossa palvelujen tuottaminen on paikoitellen jakautunut DigiHelsingin ja kaupunkiorganisaation oman toiminnan välillä. Organisoitumismuutoksista on käytännössä muodostunut noin neljän vuoden mittainen siirtymävaihe, jonka aikana työnjaossa ja vastuissa sekä henkilöstön tehtävissä on tapahtunut paljon muutoksia. Siirtymävaiheessa tehtävien ja vastuiden jako on hämärtynyt ainakin joidenkin yksityiskohtien osalta. Tällainen vastuiltaan epäselvä yksityiskohta oli tietomurrossa hyödynnetty VPN-reititin (ks. 2.1).

Tapahtumaan liittyi yksityisiä yrityksiä, joilta Helsingin kaupunki hankki tietohallinto- ja tietoturvapalveluja jo ennen tietomurtoa. Murron paljastuttua palveluita hankittiin tapahtuneen selvittämiseen ja siitä toipumiseen. Tapahtumaan liittyvät yksityiset toimijat ovat vakiintuneita ja tunnettuja ICT-alan yrityksiä.

Telia Cygate vastaa Helsingin kaupungin käytössä olleen palomuuripalvelun ylläpidosta ja lokien hallinnasta. Telia Cygate Oy:n liikevaihto vuonna 2023 oli noin 137 miljoonaa euroa ja sen henkilöstömäärä noin 400.

Fujitsu Finland Oy vastaa Helsingin kaupungille muun muassa verkko- ja pilvipalvelukapasiteetin tarjoamisesta. Lisäksi se tarjoaa palveluita kaupungin eri ICT-palveluita tarjoavien alihankkijoiden tuottamien tikettien välittämisestä ja integroinnista eri toimittajien tietojärjestelmien välillä. Fujitsu Finland Oy:n liikevaihto vuonna 2024 oli noin 300 miljoonaa euroa ja henkilöstömäärä noin 1 400.

Dustin Finland Oy suoritti KASKOn toimeksiannosta ylläpitotehtäviä verkkolaitteille. Se on päivittänyt tietomurron kohteeksi joutuneen Cisco ASA 5515 VPN-laitteen varmenteen vuosittain etähallinnan avulla. Dustin Finland Oy:n liikevaihto vuonna 2024 oli noin 165 miljoonaa euroa ja henkilöstömäärä noin 220.

Elisa Santa Monica Oy teki 3.5.2024 lähtien tietomurron teknistä tutkintaa Helsingin kaupungin tilauksesta. Yrityksen tietomurtojen tutkintatiimi antaa tukea tietomurtotapauksien selvittämiseen ja tilanteen palauttamiseen. Yritys suorittaa vuosittain useita kymmeniä vastaavia konsultointeja. Yritys tarjoaa muita myös tietoturvapalveluja, kuten verkkojen valvontapalveluja (SOC, Security Operations Center). Elisa Santa Monica Oy:n liikevaihto vuonna 2023 oli noin 64 miljoonaa euroa ja henkilöstömäärä oli noin 180.

Palo Alto Networks Oy toimitti Helsingin kaupungille palomuurit, joiden hallintapalveluista vastasi Telia Cygate. Tietomurron jälkeen Palo Alto Networks Oy analysoi palomuurien lokitietoja. Palo Alto Networks (Finland) Oy:n liikevaihto vuonna 2024 oli noin 9 miljoonaa euroa ja henkilöstömäärä noin 30.

Cisco Systems on tuottanut tietomurron jälkeen Helsingin kaupungille asiantuntijapalveluja erityisesti Cisco ASA 5515 VPN-laitteelta kerättyjen hajanaisten lokitietojen ja muistivedosten analysoinnissa. Cisco Systems Finland Oy:n liikevaihto vuonna 2024 oli noin 15 miljoonaa euroa ja henkilöstömäärä oli noin 55.

	HELSINGIN KAUPUNKIKONSERNI			KAUPUNGILLE PALVELUJA TUOTTAVAT YRITYKSET	
Toimijan nimi	**Helsingin kaupunki**	**Helsingin kaupungin toimialana KASKO**	**Palveluntuottaja DigiHelsinki**	**Useita yrityksiä**	**Yritys**
Yleis-kuvaus	Järjestämisvastuullinen toimija	Toimialakohtainen tuottamistehtävä	Kaupungin sisäisten digitaalisten peruspalvelujen tuottaminen.	Erilaisia ICT-palveluja tuottavia yrityksiä	Tietoturva-asiantuntijapalvelu
Ennen tieto-murtoa	• Tiedonhallintaympäristön kaupunkitasoinen kehittäminen. • Hallinnollinen tietoturva. • Kaupungin kokonaisarkkitehtuurin kehittäminen. • Digitaalinen perusta -ohjelman johtaminen. • DigiHelsingin konserniohjaus.	• Vastuu toimialan tiedonhallinnan toteuttamisesta ja kehittämisestä. • Tietohallinnon teknisiä vastuita, jotka eivät ole siirtyneet DigiHelsingille. • Osittain hallinnollisen ja osittain teknisen tietoturvan tehtäviä. • Epäselvyyksiä vastuujaossa DigiHelsingin kanssa erityisesti teknisen ylläpidon osalta.	• Tietoturvallisuuden hallinta ja ylläpito kaupungin ja DigiHelsingin sopimusten mukaisesti • Tietoliikenteen valvonta omassa verkossa. • Tekninen tietoturva kaupungin ja DigiHelsingin sopimusten mukaisesti • Epäselvyyksiä vastuissa KASKOn kanssa.	• Toimittavat ja ylläpitävät kaupungin tai DigiHelsingin hankkimia ict-laitteita ja palveluja. • Huolehtivat muun muassa näiden palveluiden teknisestä tietoturvallisuudesta, tietosuojasta ja jatkuvuudenhallinnasta.	Ei tuota palveluja kaupungille.
Tieto-murron aikana	• MiM työskentely alkaa. • Vastaa kaupunkitason keskitetystä viestinnästä.	• Tietomurron tunnistaminen ja torjuntatoiminnan aloittaminen. • Ilmoitukset viranomaisille, asiantuntija-avun hankinta sekä viestintä tapahtuneesta kaupunkiorganisaatiossa. • MIM työskentelyn käynnistäminen.	• Torjuntatoimenpiteiden tekniseen toteuttamiseen osallistuminen • Hyökkäyksen keskeyttäminen yhdessä KASKOn kanssa.	Havainto tietomurrosta DigiHelsingille saadaan yhden yrityksen kautta.	• Tilannekuvan muodostaminen ja avustaminen hyökkäyksen lopettamisessa. • Kaupunki tekee toimeksiannon yritykselle tietomurron paljastuttua.
Tieto-murron jälkeen	• Tilanteen hallinta ja johtaminen. • Tietoturvallisuusloukkauksen kohteena olleiden informointivelvoite. • Kehittämissuunnitelman laatiminen tietoturvallisuuden kehittämiseksi.	Toimialakohtaiset selvittämistoimenpiteet, mm. verkkolevyn sisällön selvittäminen.	Tietoturvallisuutta parantavien kehittämistoimenpiteiden esittäminen ja toteuttaminen.	• Tietomurtotutkinnassa tarvittava avustaminen esimerkiksi laitteiden forensiikkatutkinnan ja tarvittavien lokitietojen osalta. • Tietoturvapalveluiden kehittäminen.	• Uusien tarvittavien tietoturvapalveluiden tuottaminen. • Tapahtuman forensinen tutkinta ja raportointi, suositusten laatiminen.

Kuva 10. Helsingin kaupungin sisäiset ja ulkoiset toimijat sekä vastuut tietomurtotapauksessa.

2.8 Viranomaisten toiminta

Valtiovarainministeriön tehtäviin kuuluu julkisen hallinnon tietoturvallisuuden yleinen kehittäminen. Se osallistuu myös kansallisen kyberturvallisuusstrategian kehittämiseen sekä tieto- ja kyberturvallisuuden lainsäädännön kehittämiseen. Viime vuosina kehittämisen painopisteinä on ollut muun muassa yhteisten tieto- ja viestintäteknisten palveluiden häiriöhallinnan ja varautumisen kehittäminen sekä tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (Titukri). Valtiovarainministeriö kehittää julkisen hallinnon kyberturvallisuuden tilannekuvan muodostamista muiden viranomaisten ohella ja on tukemassa Digi- ja väestötietoviraston digiturvapalvelujen ja tietopalveluiden kehittämistä ja käyttöä.

Liikenne- ja viestintäministeriö

Liikenne- ja viestintäministeriö vastaa viestintäverkkojen ja palveluiden tietoturvallisuuteen liittyvästä lainsäädännöstä ja strategiatyöstä. Liikenne- ja viestintäministeriön tehtävä on mahdollistaa toimivia turvallisia ja kestäviä digitalisaation, liikenteen ja viestinnän ratkaisuja. Tavoitteena on varmistaa ja edistää kansalaisten, elinkeinoelämän ja julkishallinnon luotta-

musta tietoyhteiskunnan palveluiden turvallisuuteen. Luottamus perustuu muun muassa palveluiden helppokäyttöisyyteen, yksityisyyden suojan varmistamiseen sekä sisältöjen aitouteen.

Liikenne- ja viestintäministeriö valmistelee toimialaansa liittyvät poliittiset ja strategiset linjaukset ja lainsäädännön, minkä lisäksi ministeriö toimii aktiivisesti kansainvälisillä foorumeilla. Ministeriö huolehtii yhteyksien toimivuudesta ja turvallisuudesta, oikeudenmukaisesta vihreästä ja digitaalisesta siirtymästä sekä tiedon hyödyntämisen edellytyksistä.

Liikenne- ja viestintäministeriö vastaa yhteiskunnan turvallisuusstrategian mukaisen kyberturvallisuuden kansallisen yhteistoimintamallin ylläpidosta. Liikenne- ja viestintäministeriön hallinnonalalla toimiva Liikenne- ja viestintävirasto vastaa liikenteen ja viestinnän viranomaistehtävistä ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä sekä ylläpitää kansallisen kyberturvallisuuden tilannekuvaa.

Valtion kyberturvallisuusjohtajan toimisto on Liikenne- ja viestintäministeriöön sijoitettu, ministeriön osastoista erillinen toimintayksikkö, joka koordinoi ja yhteensovittaa kansalliseen kyberturvallisuuteen liittyviä asioita koko valtioneuvoston tasolla. Toimisto vastaa kansallisesti kyberturvallisuuden kehittämisen, suunnittelun, varautumisen ja kriittisen tieto- ja viestintäteknisen infrastruktuurin varautumisen koordinaatiosta ja yhteensovittamisesta strategisella tasolla. Se koordinoi myös Suomen kyberturvallisuusstrategian toimenpiteiden seurantaa yhdessä ministeriöiden muodostaman seurantaryhmän ja sen sihteeristön kanssa.

Kansallinen tietoturvallisuusviranomainen on Liikenne- ja viestintäministeriön hallinnonalalla toimiva **Liikenne- ja viestintävirasto Traficom**. **Kyberturvallisuuskeskus** kuuluu osaksi Liikenne- ja viestintävirasto Traficomia ja sen tehtävistä säädetään Liikenne- ja viestintävirastosta annetussa laissa[38].

Kyberturvallisuuskeskus tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. Kyberturvallisuuskeskus toimii julkisesti säännellyn satelliittipalvelun vastuuviranomaisena ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/887 6 artiklan mukaisena kansallisena koordinointikeskuksena. Lisäksi Kyberturvallisuuskeskus huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo sähköisen viestinnän toimintavarmuutta sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin. (19.11.2021/1002)

Tämän ohella Traficomin kyberturvallisuuteen liittyvistä tehtävistä säädetään sähköisen viestinnän palveluista annetun lain (917/2014) 304.1 §:ssä, jonka 1, 7, 8 ja 10 kohtien mukaan sen lisäksi, mitä muualla laissa säädetään, Liikenne- ja viestintäviraston tehtävänä on:

1) edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja turvallisuutta;

[38] 936/2012.

7) kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista;

8) tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta;

10) selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia;

Näihin lakisääteisiin tehtäviin perustuen CERT-toiminnon lakisääteisenä tehtävänä on myös koostaa ja jakaa kansallista kyberturvallisuuden tilannekuvaa tietoturvaloukkausten selvittämiseksi sekä ennaltaehkäisemiseksi.

Kyberturvallisuuskeskus vastaanottaa lakisääteisten tehtäviensä hoitamiseksi vapaaehtoisia tietoturvaloukkausilmoituksia, jotka luokitellaan poikkeaman merkittävyyden ja vaikutusten laajuuden perusteella. Luokittelun tarkoituksena on suorittaa ensiarvio siitä, miten kriittinen poikkeama on ja kuinka nopeasti siihen tulisi ilmoittajan antamien tietojen valossa reagoida. Lisäksi ilmoitusten perusteella se kykenee varoittamaan muita toimijoita, jotta nämä pystyvät parantamaan oman kyberturvallisuutensa tasoa.

Kyberturvallisuuskeskus toimii kansallisena koordinointikeskuksena[39] ja kansallisena NIS-koordinaatiopisteenä eri viranomaisten välillä. Tehtävä laajeni 8.10.2024 voimaan tulleen NIS 2 -direktiivin[40] toimeenpanon osalta 8.4.2025 voimaan astuneella kyberturvallisuuslailla.[41]

Kyberturvallisuuslailla[42] säädetään Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen CSIRT-yksikön kyberturvallisuuteen liittyvistä tehtävistä. Kyberturvallisuuslain 20.1 §:n mukaan CSIRT-yksikön tehtävänä on muun muassa reagoida poikkeamailmoituksiin ja tarvittaessa avustaa poikkeamasta ilmoittanutta tahoa poikkeaman käsittelyssä sekä kerätä ja analysoida uhkatietoja ja tietoturvaloukkausten tutkintaa koskevia tietoja. Lisäksi kyberturvallisuuslaissa säännellään aiempaa seikkaperäisemmin Kyberturvallisuuskeskuksen HAVARO ja Hyöky -palvelujen tuottamiseen liittyvistä lakisääteisistä tehtävistä ja toimivaltuuksista.

Edellisten lisäksi sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 303.1 §:n mukaan Liikenne- ja viestintäviraston tehtävänä on valvoa tämän lain sekä sen nojalla annettujen säännösten ja päätösten noudattamista, jollei tässä laissa muuta säädetä.

SVPL:ssä säädetään muun muassa teleyritysten, yhteisötilaajien ja muiden viestinnän välittäjien sähköisen viestinnän käsittelyyn liittyvistä tietoturvallisuusvelvoitteista. Lisäksi SVPL:ssä ja sen nojalla annetuissa määräyksissä on lukuisia teletoiminnan tietoturvallisuutta ja varautumista koskevia vaatimuksia. Traficomin sisällä Kyberturvallisuuskeskuksen Ohjaus- ja valvontaosasto vastaa näihin säännöksiin ja niiden nojalla annettuihin määräyksiin liittyvästä toimijoiden ohjauksesta ja valvonnasta.

Lisäksi Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on julkishallinnon toimialan, digitaalisen infrastruktuurin toimialan tiettyjen toimijoiden, tutkimusorganisaatioiden, digitaalisen palvelun tarjoajien sekä ICT-palveluiden hallintaa tarjoavien toimijoiden valvova viranomainen NIS2-/kyberturvallisuusdirektiiviin perustuvan kansallisen kyberturvallisuuslain mukaisesti.

---

[39] Euroopan parlamentin ja neuvoston asetus Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta (EU) 2021/887.
[40] Euroopan unionin direktiivi NIS 2 eli Network and Information Security Directive (verkko- ja tietoturvadirektiivi).
[41] HE 243/2022.
[42] 124/2025.

Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa kyberturvallisuuden tilannekuvaa. Keskus julkaisee kuukausittaista Kybersää-raporttia sekä ajankohtaisia tapahtumia käsittelevää viikkokatsausta.

Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa. Tilannekuvan muodostamisessa hyödynnetään Traficomin koko liikenne- ja viestintäsektorin toimialaa sekä kansallisten lähteiden, kuten huoltovarmuuskriittisten organisaatioiden verkostoja ja turvallisuusviranomaisia. Lisäksi hyödynnetään virallisia tai vapaaehtoisuuteen sekä molemminpuoliseen luottamukseen perustuvia kansainvälisiä yhteistyöverkostoja.

Hyöky-palvelu[43] on Kyberturvallisuuskeskuksen tarjoama palvelu julkisen hallinnon organisaatioille ja yhteiskunnan toiminnan kannalta kriittisille toimijoille niiden julkisen verkon hyökkäyspinnan kartoittamiseksi. Hyöky-palveluun liittyvä asiakas ilmoittaa käyttämänsä IP-osoiteavaruudet, johon tietoturvakartoitus kohdistetaan. Hyöky-raportteja toimitetaan tilaajalle muutaman kuukauden välein tai tarpeen mukaan.

Helsingin kaupungista tuli Hyöky-palvelun asiakas vuoden 2023 lopussa. Tutkinnassa tarkasteltiin neljää Hyöky-raporttia, vuosilta 2023–2024. Raporteissa nousi esille kriittisiä ja korkean riskin haavoittuvuuksia.

Ensimmäiseen kartoitukseen ilmoitettiin KASKOlta vain julkisten palveluiden IP-avaruus. Tällä haluttiin varmistaa, etteivät porttiskannaukset aiheuta epätoivottuja sivuvaikutuksia, kuten aiheettomia varoituksia verkkohyökkäyksistä. Tietomurron kohteeksi joutunutta VPN-reititintä ei laskettu kuuluvaksi julkisten palveluiden IP-avaruuteen, joten sen IP-osoite jätettiin pois kartoituksesta.

Jos VPN-reititin olisi ollut mukana kartoituksessa, se olisi näkynyt raportissa havaittuna laitteena. Skannaus olisi listannut palvelimen, mistä KASKO olisi voinut havaita, että verkossa on ulospäin näkyvä ”unohtunut” laite.

Kyberturvallisuuskeskus toteutti yhdessä Helsingin kaupungin kanssa tietomurron selvittämisen yhteydessä ulkoisten Hyöky-skannausten ohella muitakin kattavampia sisäisiä skannauksia Helsingin kaupungin ympäristöön erilaisilla skannaustyökaluilla. Kyberturvallisuuskeskus muun muassa varmisti yhteistyössä Helsingin kaupungin eri toimialojen kanssa, että kaikki käytössä olevat IP-osoitelohkot ovat tiedossa. Lohkoihin tehtiin useita skannauksia muiden mahdollisesti haavoittuvien kohteiden havaitsemiseksi. Lisäksi skannausten avulla pyrittiin selvittämään, oliko hyökkääjä päässyt laajentamaan pääsyään kaupungin muiden toimialojen verkkoalueisiin, oliko hyökkääjä vielä aktiivisena kaupungin verkkoympäristössä ja löytämään hyökkääjän mahdollisesti asentamia takaportteja.

Kyberturvallisuuskeskus suoritti erillisen skannauksen Suomen IP-osoiteavaruudesta selvittääkseen, onko muilla organisaatioilla käytössä vastaavia vanhentuneita ja haavoittuvia VPN-laitteita.

Havaro (HAvainnointi ja VAROitus) on palvelu, joka on tarkoitettu havaitsemaan ja varoittamaan ennakolta vakavista tietoturvaloukkauksista. Kyseistä tietoturvapalvelua tuottaa Liikenne- ja viestintävirasto (Traficom). Havaro tarkkailee asiakasorganisaation tietoliikennettä ja etsii merkkejä kehittyneistä hyökkäyksistä, kuten valtiollisista vakoiluohjelmista ja APT-toiminnasta (Advanced Persistent Threat).

[43] Hyökkäyspinta-alan kartoituspalvelu.

Palvelu hankitaan kaupalliselta tietoturvan palvelukeskukselta (SOC) ja sen toiminnasta vastaa Kyberturvallisuuskeskus yhdessä alan kaupallisten toimijoiden asiantuntijoiden kanssa. Yhteiskunnan toiminnan kannalta tärkeät huoltovarmuuskriittiset toimijat sekä julkisen hallinnon toimijat voivat ottaa HAVARO-palvelun käyttöön sijoittamalla sen edellyttämän oman sensorilaitteiston tai ohjelmiston omaan IT-ympäristöönsä. Sensorit pyrkivät havaitsemaan uhkaavaa liikennettä ja varoittamaan siitä. HAVARO-palvelun tuottamaa dataa käytetään Kyberturvallisuuskeskuksessa merkittävien kyberpoikkeamien selvittämiseen ja kansallisen kyberturvallisuuden tilannekuvan muodostamiseen.

CERT-toiminto (Computer Emergency Response Team) on Kyberturvallisuuskeskuksen toiminto, jonka tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturvaasioista. Lisäksi toiminto auttaa vakavien tietoturvaloukkausten teknisessä selvittämisessä.

Tietoturvailmoitus tietoturvaloukkauksista tehdään Kyberturvallisuuskeskukselle verkkolomakkeella. Ilmoitukset tilastoidaan ja luokitellaan. Yhtenä luokitteluperusteena on se, kuinka suureen joukkoon ihmisiä ja toimijoita poikkeama vaikuttaa, kuinka tärkeä kohde on yhteiskunnallisesti ja kuinka välittömiä toimenpiteitä tarvitaan. Luokittelun jälkeen arvioidaan, millaisiin toimenpiteisiin ilmoituksen perusteella tarvitsee mahdollisesti ryhtyä.

Kyberturvallisuuskeskus on toimintavalmiudessa kaikkina vuorokauden aikoina. Yöaikana päivystys on toteutettu varallaolojärjestelyllä, joka pystyy tarvittaessa reagoimaan vakaviin tilanteisiin.

Kyberturvallisuuskeskuksen rooli tietoturvaloukkauksissa rajoittuu lähinnä kohteeksi joutuneen toimijan avustamiseen ja tukemiseen. Annettavan avun ja tuen tarkoituksena on neuvonnalla edistää tietoturvaloukkauksen selvittämistä, torjuntaa ja siitä palautumista. Annettavan avun tai tuen laajuutta ei ole etukäteen määritetty, vaan siihen vaikuttavat muun muassa kyseisellä hetkellä käytettävissä olevat resurssit. Lisäksi asiaan vaikuttaa se, missä määrin toimija itse on kykenevä hoitamaan ja selvittämään asiaa. Lakisääteisten tietoturvaloukkausten selvittämistehtäviensä hoitamiseksi poikkeuksellisissa tapauksissa, kuten Helsingin kaupungin tietomurrossa, Kyberturvallisuuskeskuksen asiantuntijat voivat avustaa asiakasta myös tietoturvaloukkauksen konkreettisessa käsittelyssä (DFIR, Digital Forensics & Incident Response).

Tietoturvaloukkausten kohteena voi olla hyvin vaihtelevin resurssein olevia toimijoita, jonka takia viranomaisavun tarve voi vaihdella ennakoimattomasti. Kyberturvallisuuskeskuksessa ei kyseisen tietomurtotapauksen tapahtuman aikaan ollut yleistä tietomurtotapauksien selvittämiseen prosessikuvausta.

Valmius tietoturvaloukkausten selvittämiseen ja torjumiseen perustuu Suomessa laaja-alaiseen viranomaisten ja tietoturvayritysten sekä muiden toimijoiden väliseen yhteistyöhön ja tietojenvälitykseen. Kyberturvallisuuskeskus toimii toimintaa kokoavana ja edistävänä tahona. Sen avustuspalvelut ovat uhriksi joutuneelle organisaatiolle maksuttomia.

Kansalliseen kyberturvallisuuden koordinointiin liittyen Kyberturvallisuuskeskus koordinoi ISAC-tiedonvaihtoryhmiä[44], jotka ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-ryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä. Tarjolla on omat ryhmät myös kunnille ja valtionhallinnolle.

[44] ISAC-tiedonvaihtoryhmät, Information Sharing and Analysis Centre
https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Opetushallitus on opetus- ja kulttuuriministeriön alainen virasto, joka vastaa koulutuksen ja varhaiskasvatuksen kehittämisestä, ohjauksesta ja arvioinnista. Sen tehtäviin kuuluu opetussuunnitelmien ja tutkintojen perusteiden laatiminen, koulutuspoliittisten tavoitteiden toteuttaminen sekä koulutuksen laatua ja yhdenvertaisuutta edistävien toimien kehittäminen. Opetushallitus tukee oppilaitoksia, opettajia ja oppilaita tarjoamalla ohjeita, materiaaleja ja rahoitusta. Lisäksi se vastaa koulutuksen kansainvälisestä yhteistyöstä ja osallistuu Suomen koulutusjärjestelmän kehittämiseen.

Opetushallitus on laatinut opetus- ja sivistyshallinnolle laajasti ohjeistusta koulujen ja päiväkotien tietojen käsittelystä, tietosuojasta ja tietoturvallisuudesta. Materiaalia on laadittu yhdessä tietosuojavaltuutetun kanssa. Tietosuojavaltuutettu on 15.10.2021 tehnyt Opetushallitukselle aloitteen opetuksessa käytettävien tietojärjestelmien henkilötietojen käytön kehittämiseksi. Aloitteen mukaiset toimenpiteet ovat kesken.

Tiedonhallintalautakunta on valtiovarainministeriön yhteyteen perustettu erityisviranomainen, jonka tehtävänä on arvioida ja edistää tiedonhallintalaissa säädettyjen vaatimusten ja menettelytapojen toteuttamista. Tiedonhallintalautakuntaan kuuluu edustajia julkisesta hallinnosta. Siinä on edustettuna keskeiset tiedonhallintaa ohjaavat viranomaiset sekä tiedonhallintalakia soveltavia viranomaisia. Tiedonhallintalautakunta laatii kerran kahdessa vuodessa arviointiraportin sen toteuttamien arviointien tuloksista ja tekee raportissaan suosituksia, jotka se osoittaa valtiovarainministeriölle. Tiedonhallintalautakunnan toimivaltaan ei myöskään kuulu arvioida tiedonhallintalain 4 luvussa säädettyjen tietoturvallisuusvaatimusten toteuttamista.

Tiedonhallintalautakunta on antamassaan arviointikertomuksessa kiinnittänyt huomiota siihen, että tiedonhallinnan ohjaustehtävät jakautuvat useille eri viranomaisille ja niissä on päällekkäisyyksiä.[45] Tiedonhallintalautakunnan lisäksi tietoturvallisuutta ohjaavia suosituksia tai parhaita käytäntöjä jakavat ainakin Kyberturvallisuuskeskus, Huoltovarmuuskeskus ja Digi- ja väestötietoviraston digiturvapalvelut. Lisäksi aihealueeseen liittyviä tehtäviä on ulkoministeriöllä, Huoltovarmuuskeskuksella ja Kansallisarkistolla.

[45] Tiedonhallintalautakunnan arviointikertomus 2022–2023 s. 42. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165453/VM_2024_16.pdf

Kuva 11. Tiedonhallinnan yleislainsäädännön ohjaukseen liittyvät viranomaiset. (Kuva: Tiedonhallintalautakunta)

Tiedonhallintalautakunta arvioi Helsingin kaupungin toimintaa vuosina 2020–2023 osana normaalia kuntakenttään kohdistettua valvontasuunnitelman mukaista työtään. Valvonta on luonteeltaan laillisuusvalvontaa ja sitä toteutetaan lähinnä tietopyynnöillä ja kyselyillä. Varsinaista valvontakäyntiä Helsingin kaupungille ei suoritettu. Tehtyjen arviointien perusteella Helsingin kaupungin tiedonhallintalain velvoitteiden noudattamisessa ei havaittu puutteita.

Helsingin poliisilaitos on Suomen suurin poliisiyksikkö. Siinä työskentelee noin 1 600 henkilöä, joista poliiseja on noin 1 300. Yksikkö toimii Helsingin kaupungin alueella ja vastaa paikallispoliisin tehtävistä. Sen lisäksi yksikkö vastaa tasavallan presidentin, valtioneuvoston jäsenten sekä valtiovieraiden turvallisuudesta. Myös poliisin valtakunnallinen valmiusyksikkö Karhu, valtakunnallinen ihmiskauppatutkintaryhmä sekä liikenneturvallisuuskeskus on sijoitettu Helsingin poliisilaitokselle.

Poliisilaitos vastaa alueellaan tapahtuneiden rikosten esitutkinnasta, jos poliisin työjaosta ei muuta johdu. Helsingin poliisilaitos otti vastaan Helsingin kaupungin tekemän rikosilmoituksen sähköisen ilmoitusjärjestelmän kautta. Rikosilmoitus esikäsiteltiin ja sille määritettiin tutkija ja tutkinnanjohtaja.

Poliisilaitos suoritti esitutkintatoimenpiteinä muun muassa tiedonhankintaa Helsingin kaupungilta sekä julkaisi esitutkinnan aloittamista koskevan tiedotteen. Poliisilaitos aloitti myös yhteistyön keskusrikospoliisin kanssa.

Keskusrikospoliisi (KRP) on Suomen poliisihallinnon valtakunnallinen erikoisyksikkö, jonka toimialueena on koko Suomi. Keskusrikospoliisissa on erityisosaamista esimerkiksi järjestäytyneen rikollisuuden, huumausainerikollisuuden, talousrikollisuuden ja kyberrikollisuuden torjunnassa. Se toimii kansainvälisessä yhteistyössä muiden maiden viranomaisten kanssa ja koordinoi Suomen osallistumista Europolin ja Interpolin toimintaan.

Keskusrikospoliisi tukee paikallispoliisia monimutkaisissa rikostutkinnoissa ja vastaa osaltaan maan turvallisuuden ylläpitämisestä.

Keskusrikospoliisi tekee yhteistyötä paikallispoliisin kanssa niin, että paikallispoliisi huolehtii asiaomistajiin liittyvistä asioista ja keskusrikospoliisi tekniseen tutkintaan sekä kansainväliseen yhteistyöhön liittyvistä asioista. Tutkinnan yleisjohtaja on Keskusrikospoliisista.

Keskusrikospoliisin toimenpiteet Helsingin tietomurrossa liittyvät esitutkintaan. Näiltä osin poliisin toiminta tietoverkkorikoksissa poikkeaa muista rikoslajeista, sillä poliisin mahdollisuudet rikoksen keskeyttämiseksi tietoverkossa ovat varsin rajoitetut.

Murron havaitsemisen jälkeen muiden toimijoiden pelastustoimenpiteet palauttivat KASKOn verkon turvalliseen tilaan. Poliisilla ei ole toimintaedellytyksiä ottaa haltuun verkkoympäristöjä, aloittaa niiden valvontaa tai poistaa tunkeutujaa verkosta. Tällaiset toimet ovat hyökkäyksen kohteeksi joutuneen organisaation tai sen käyttämien palvelutuottajien varassa.

Tietoverkkorikoksien selvittämiseen ja rikosvastuun toteuttamiseen vaatii yleensä merkittävästi kansainvälistä yhteistyötä ja kontakteja, jotka ovat Keskusrikospoliisin vastuulla.

KRP ilmoitti 13.3.2025 epäilevänsä Helsingin kaupungin tietomurtoon liittyvän tietosuojarikoksen, jonka esitutkinnan se aloitti. Tutkinnassa selvitetään, oliko kaupunki suojannut tietoja asianmukaisesti.

Suojelupoliisi (Supo) ennaltaehkäisee ja torjuu kaikkein vakavimpia kansallisen turvallisuuden uhkia, kuten terrorismia ja vieraiden valtioiden Suomeen kohdistamaa laitonta tiedustelua. Korona-pandemian ja digitalisoitumisen myötä yritysten ja yhteiskunnan toiminnot ovat siirtyneet yhä enemmän verkkoon, jolloin myös verkon rooli Suojelupoliisin tiedustelutoiminnassa on kasvanut. Tietomurron selvityksessä Suojelupoliisi lähinnä seurasi esitutkinnan etenemistä.

Tietosuojavaltuutettu (TSV) on itsenäinen viranomainen, jonka tehtävänä on valvoa henkilötietojen käsittelyä ja varmistaa, että tietosuoja-asetusta ja muuta henkilötietojen käsittelyä koskevaa erityislainsäädäntöä noudatetaan. Tietosuojavaltuutettu neuvoo tietosuoja-asioissa, käsittelee tietosuojarikkomuksiin liittyviä valituksia ja voi määrätä seuraamusmaksuja. Tietosuojavaltuutetulla on oikeus tarkastaa organisaatioiden tietosuojakäytäntöjä. Tietosuojavaltuutetun toimistossa työskentelee tietosuojavaltuutetun lisäksi kaksi apulaistietosuojavaltuutettua sekä noin 60 muuta virkahenkilöä.

Havaitessaan tietoturvaloukkauksen rekisterinpitäjä on velvollinen tekemään siitä ilmoituksen tietosuojavaltuutetulle 72 tunnin kuluessa. Tietosuojavaltuutetun toimisto aloittaa tapauksen selvittämisen ilmoituksen perusteella.

Tietosuojavaltuutettu on selvittänyt Helsingin tietomurtotapahtumaa hallintoasian käsittelysäännösten perusteella ja tulee antamaan asiassa ratkaisun myöhemmin. Tietosuojavaltuutetun toteuttama valvonta on luonteeltaan laillisuusvalvontaa ja sitä toteutetaan hallintoasian käsittelyprosessissa hallintolain määräämässä järjestyksessä.

Tietosuojavaltuutettu sai Helsingin kaupungin tekemän ilmoituksen tietoturvaloukkauksesta tietomurron paljastuttua 30.4.2024, minkä perusteella tietosuojavaltuutetun toimisto aloitti asian selvittämisen. Helsingin kaupunki täydensi ilmoitustaan useita kertoja sisäisten tutkintatoimien edistyttyä ja tietosuojavaltuutetun toimiston pyytämien lisäselvitysten perusteella. Tietosuojavaltuutettu antoi Helsingin kaupungille neuvontaa tietosuoja-

asetuksen noudattamiseen liittyvissä asioissa, kuten tietomurtoon liittyvän informointivelvollisuuden toteuttamisessa.

Tietosuojavaltuutettu on edellä kerrotun lisäksi tukenut Helsingin kaupungin viestinnällisiä toimia sekä ottanut vastaan yhteydenottoja ihmisiltä, joiden tietoja on saattanut olla tietomurtoon sisältyneessä aineistossa.

Suomen Kuntaliitto ry on kuntien muodostama rekisteröity yhdistys, jonka toiminnassa ovat mukana myös maakuntien liitot, kuntayhtymät ja kuntataustaiset osakeyhtiöt. Kuntaliitto on kuntakentän yhteinen edunvalvoja, jonka organisaatiossa työskentelee noin 140 henkilöä. Kuntaliiton tytäryhtiöitä ovat FCG Finnish Consulting Group Oy, KL-Kuntahankinnat Oy sekä KL-Kustannus Oy. Kuntaliiton edunvalvonta kattaa kaikki kuntakenttää koskevat asiat. Niihin sisältyvät myös kuntien varhaiskasvatuksen, perusopetuksen ja toisen asteen koulutuksen sekä digitalisaation, kyberturvallisuuden ja tietosuojan kysymykset. Kuntaliitto tukee kuntien tiedonhallinnan, tietoturvan ja tietosuojan vertaiskehittämistä ja -verkostoitumista esimerkiksi ylläpitämällä kuntien tietoturva- ja tietosuojavastaavien ja tiedonhallinnan verkostoja sekä tarjoamalla neuvontaa jäsenilleen. Lisäksi FCG järjestää kuntakentälle maksullisia digitaalisen turvallisuuden ajankohtaistapahtumia ja koulutuksia.

Viranomaisten ennalta estävässä toiminnassa korostuu ohjaava ja neuvova toiminta, jolla pyritään huolehtimaan siitä, että toiminnanharjoittaja on tunnistanut keskeiset henkilötietojen käsittelyn ja tiedonhallinnan vastuut. Säännönmukaista valvontatoimintaa näiden velvoitteiden toteuttamiseen kohdistetaan vain hyvin rajallisesti. Tiedonhallintalautakunnan valvontatyö pyrkii lähinnä kuvailemaan tiedonhallintavelvoitteiden toimeenpanoa valtakunnallisesti. Tietosuojavaltuutettu toteuttaa suunniteltuja ja ennakkoon ilmoittamattomia valvontakäyntejä. Vastuiden noudattaminen voi tulla lähinnä jälkikäteen arvioitavaksi erilaisten tietosuojaloukkausten yhteydessä tai toiminnasta tehtävien kantelujen kautta.

Julkisin varoin ylläpidettävillä Hyöky- ja Havaro-palveluilla on pystytty tunnistamaan ja estämään uhkia ja haavoittuvuuksia, joita sitä käyttävä organisaatio tai sen käytössä ollut tietoturvapalveluntarjoaja ei ole huomannut. Palvelut eivät kuitenkaan ole käytössä laaja-alaisesti julkisella sektorilla. Palveluissa on myös teknistä kehittämistarvetta.

Rikosten torjunnassa keskeisiä ovat toimenpiteet, joilla estetään rikoksia ennakolta sekä varmistetaan rikosvastuun toteutuminen. Nämä toimenpiteet edellyttävät kansainvälistä yhteistyötä. Merkittäviä ovat myös kansalliset verkkorikollisuuden torjunnan kehittämishankkeet.

Tietomurtotapahtuman hallinnan keskiössä on se organisaatio, jonka hallussa oleviin tietoihin tietomurto kohdistuu. Tämä edellyttää, että organisaatiolla on tietoriskeihin nähden oikeasuhtaiset tekniset ja hallinnolliset suojauskeinot sekä kyky havaita ja torjua alkava tietomurto. Lisäksi organisaation on etukäteen varmistettava, että sillä on tarvittaessa käytössään tarvittavaa osaamista tietomurron torjuntaan, selvittämiseen ja häiriötilanteen hallintaan. Myös tietomurron uhrien informointi on tietoja hallinneen organisaation vastuulla.

Organisaatio voi etukäteisvalmisteluin huolehtia, että sillä on saatavilla riittävän asiantuntevaa apua tietomurron selvittämiseksi ja hallitsemiseksi. Suomessa on useita tällaisia DFIR-palveluja (Digital Forensics & Incident Response) tarjoavia yrityksiä. Rikosasian selvittämiseksi tarvitaan organisaation ja tietojärjestelmäympäristön tuntemusta, jota esitutkintaviranomaisilla ei ole. Siksi organisaation itsensä tekemät tai yrityksiltä hankkimat selvitykset ovat keskeisessä roolissa rikoksen selvittämisessä.

Tietomurtotapahtuman selvittämiseen osallistuu omien tehtäviensä mukaisesti useita eri viranomaisia (paikallisesti, kansallisesti ja kansainvälisesti). Tietomurron kohteeksi joutuneen tukemiseksi laajinta maksutonta asiantuntija-apua antaa Kyberturvallisuuskeskus.

Tietomurtotapahtumiin ei ole lainsäädännössä määrätty johtavaa viranomaista samalla tavoin kuin reaalimaailmassa tapahtuviin onnettomuuksiin ja rikoksiin, joissa yleisjohto vastuu jakautuu tyypillisesti pelastus- tai poliisiviranomaiselle. Häiriötilanteen hallinnan malli poikkeaa edellä mainitusta ja noudattaa riskienhallinnassa vastuunjakoa, jossa toimija vastaa myös poikkeama- ja häiriötilanteiden käsittelystä varsin itsenäisesti.

Kyberturvallisuuden kansallinen yhteistoimintamalli Suomessa on hajautettu ja vastaa periaatteiltaan kokonaisturvallisuuden yhteistoimintamallia. Kyberturvallisuuden yhteistoimintamallissa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Kyberturvallisuuden yhteistoimintamallin ylläpitäminen on yksi yhteiskunnan turvallisuusstrategian strategisista tehtävistä ja sen tavoitteena on varmistaa kaikissa oloissa yhteiskunnan keskeisten toimijoiden tiivis yhteistyö varautumisessa.

Kyberturvallisuutta koskeviin kriisitilanteisiin laaditaan kyberturvallisuuslain myötä laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelma, jossa yksilöidään käytettävissä olevat valmiudet, voimavarat ja menettelyt. Näihin sisältyvät myös tarpeelliset tiedot viranomaisten tehtävistä ja vastuista.

Yhteiskunnan elintärkeitä toimintoja uhkaavien häiriötilanteiden hallinta nojautuu kokonaisturvallisuuden mallin mukaisesti mahdollisimman kattavaan yhteistyöhön viranomaisten, paikallishallinnon, eri hallinnonalojen ja ministeriöiden sekä elinkeinoelämän välillä ja muiden turvallisuustoimijoiden tukemiseen. Tämä malli pätee myös kyberpoikkeaman hallinnassa, jossa usealla viranomaisella on tehtäviä poikkeaman vaiheesta riippuen. Traficomin Kyberturvallisuuskeskus vastaa sille ilmoitetun kyberpoikkeaman ensi vaiheessa poikkeaman selvittämisestä ja toimenpiteiden koordinoinnista. Siinä vaiheessa, kun kyberpoikkeaman kohteeksi joutunut organisaatio tekee asiasta rikosilmoituksen, asian johto- ja selvittämisvastuu siirtyy poliisille. Toimivaltainen viranomainen johtaa operatiivista toimintaa, käynnistää häiriötilanteen hallintaan liittyvät toimenpiteet, vastaa viestinnästä ja tiedottaa tilanteesta sovittujen käytäntöjen mukaisesti.

Kyberturvallisuustapahtumien torjuntaa koskevassa lainsäädännössä on tapahtumassa muutoksia. Esimerkiksi viranomaisten yhteistyötä laaja-alaisissa kyberturvallisuuspoikkeamien ja kriisien hallinnassa tullaan tarkastelemaan uudelleen.

	LIIKENNE- JA VIESTINTÄMINISTERIÖN HALLINNON ALA	SISÄMINISTERIÖN HALLINNON ALA			MUUT VIRANOMAISET
Toimijan nimi	**Traficomin Kyberturvallisuuskeskus**	**Helsingin poliisilaitos**	**Keskusrikospoliisi**	**Supo**	**Tietosuojavaltuutetun toimisto**
Yleis-kuvaus	Kyberturvallisuuskeskuksen CERT-toiminnon (Computer Emergency Response Team) tehtävänä on ennalta-ehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista.	Esitutkintaviranomaiset		Kansallinen turvallisuus	Kansallinen tietosuojaviranomainen
Ennen tieto-murtoa	• Tilannekuva- ja verkostopalvelut, havainnointi ja avunanto. • Ylläpitää kumppanuuksia ja kansainvälisiä suhteita tehtäviensä hoitamiseksi. • Hyöky - jatkuvat skannaukset sekä raportointi hyökkäys-pinnan kartoittamiseksi ja ennaltaehkäisyä varten. • HAVARO - jatkuva vakavien tietoturvauhkien havainnointi asiakkaan ympäristössä.		• Hankkeet verkko-rikollisuuden ennalta-ehkäisemiseksi. • Kansainvälinen tietojen vaihtaminen ja rikollisuuden torjunta.	Havaita, estää ja paljastaa sellaisia toimia, hankkeita ja rikoksia, jotka voivat uhata valtio- tai yhteis-kuntajärjestystä tai Suomen sisäistä tai ulkoista turvallisuutta.	Valvoa tietosuojalainsäädännön ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista, edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista, velvollisuuksista ja oikeuksista, tehdä selvityksiä ja tarkastuksia määrätä hallinnollisia seuraamuksia tietosuoja-asetuksen rikkomisesta.
Tieto-murron aikana	• Kohteeksi joutuneen organisaation tukeminen ja asiantuntija-avun antaminen. • HAVARO - tietomurron havaitseminen ja vastatoimenpiteiden käynnistäminen.	• Rikosilmoituksen vastaanottaminen aluevastuuperiaatteen mukaisesti. • Esitutkinnan käynnistäminen. • Yhteistyö KRP:n kanssa.	Esitutkintaan osallistuminen ja sen tukeminen	Tilanteen vaatiessa tarvittava asiantuntija-apu.	• Henkilötietojen tietoturva-loukkausilmoituksen vastaanottaminen. • Tilanteen vaatiessa tarvittava asiantuntija-apu.
Tieto-murron jälkeen	• Hyöky-skannausten toteuttaminen. • Tietojen välittäminen ja kokoaminen kansallisesti ja kansainvälisesti. • Tietoturvallisuustoimen-piteiden kehittämis-ehdotusten antaminen. • HAVARO - tietomurron tutkinnan ja palautumisen tukeminen. • Tarvittaessa DFIR-tutkintatoimet.	• Esitutkinnan suorittamis-velvollisuus. • Tutkintatoimet. • Yhteydenpito tietomurron asianomistajiin. • Esitutkinnan johtaminen siirretty KRP:lle.	• Kansainvälisen ulottuvuuden kysymykset rikoksen tekijän tunnistamiseksi ja tavoittamiseksi. • Forensiset tutkintatoimet. • Viestintä tapahtuman tutkintaan liittyen.	Tietomurron merkitys kansalliselle turvallisuudelle.	• Tietoturvallisuusloukkauksen uhrien oikeuksen valvontatoiminta. • Määrätä mahdollisia hallinnollisia seuraamuksia tietosuoja-asetuksen rikkomisesta.

Kuva 12. Julkiset toimijat ja viranomaiset sekä vastuut tietomurtotapauksissa.

2.9 Säädökset, määräykset ja ohjeet

Tässä luvussa käsitellään Helsingin kaupungin ulkopuolisten toimijoiden antamia määräyksiä, ohjeita ja suosituksia.

Kuntalain[46] 8 §:n mukaan kunnalla on järjestämisvastuu sille laissa säädetyistä tehtävistä. Vastuu kattaa yhdenvertaisen saatavuuden varmistamisen, tarpeen, määrän ja laadun määrittämisen, tuottamistavan valinnan, tuottamisen valvonnan sekä julkisen vallan käytön ja tehtävien rahoitusvastuun.

Helsingin kaupunki on kuntalain mukaisessa vastuussa varhaiskasvatuksen, perusopetuksen, lukio-opetuksen ja ammatillisen koulutuksen järjestämisestä. Tehtävistä on säädetty tarkemmin erityislainsäädännössä kuten varhaiskasvatuslaissa[47], perusopetuslaissa[48], lukiolaissa[49] ja ammatillisesta koulutuksesta annetussa laissa[50].

[46] 410/2015.
[47] 540/2018.
[48] 628/1998.
[49] 714/2018.
[50] 531/2017.

Suomen perustuslain[51] 2 §:n 3 momentissa säädetään hallinnon lainalaisuusperiaatteesta, jolla turvataan viranomaisessa asioivien oikeuksia. Sen mukaan julkisen vallan käytön on perustuttava lakiin ja kaikessa julkisessa toiminnassa on myös noudatettava lakia tarkoin. Lakisääteisissä palveluissa hallinnon asiakkaan mahdollisuudet vaikuttaa oman asiansa tai omien tietojensa käsittelyyn ovat kuitenkin rajalliset ja siksi viranomaisen toimet oikeusturvan toteuttamisessa keskeisiä.

Hallinnon lainalaisuutta korostaa perustuslain 118 §:ssä säädetty virkavastuu, jonka mukaan jokainen virkamies vastaa virkatoimiensa lainmukaisuudesta. Tätä virkavastuuta täydentää rikoslaki[52], jonka luvussa 40 säädetään virkarikoksista, joihin kuuluvat muun muassa 40. luvun 9 §:ssä tarkoitettu virkavelvollisuuden rikkominen sekä 10 §:n mukainen tuottamuksellinen virkavelvollisuuden rikkominen. Tietosuojalakia[53] säädettäessä hallinnon lainmukaisuusvaatimusta ja virkahenkilön virkavastuuta pidettiin yhtenä perusteena sille, ettei hallinnollista seuraamusmaksua ulotettu viranomaisiin.[54]

Hallintolain[55] toisessa luvussa säädetyillä hyvän hallinnon perusteilla turvataan viranomaisten kanssa asioivien ihmisten oikeuksia, joita ovat muun muassa vaatimus hallinnossa asioivien tasapuolisesta ja puolueettomasta kohtelusta sekä viranomaisen toimivallan käyttämisestä yksinomaan lain mukaan hyväksyttäviin tarkoituksiin. Muita vaatimuksia ovat palveluperiaate, tiedottamisvelvollisuus, neuvontatyö, asiallisen ja selkeän kielenkäytön vaatimus sekä viranomaisten yhteistyö. Hallinnon asiakkaita turvataan myös hallintolain menettelysäännöksillä sekä mahdollisuudella valittaa päätöksistä tai tehdä hallintokantelu. Lisäksi eduskunnan oikeusasiamies ja oikeuskansleri valvovat viranomaisten ja virkahenkilöiden toiminnan lainmukaisuutta sekä sitä, että viranomaiset ja virkahenkilöt täyttävät velvollisuutensa.

Kuntalain[56] 90 §:n mukaan jokaisessa kunnassa ja kuntayhtymässä on oltava hallintosääntö. Hallintosäännössä annetaan lain mukaan tarpeelliset määräykset ainakin kunnan hallinnon ja toiminnan järjestämisestä, päätöksenteko- ja hallintomenettelystä sekä valtuuston toiminnasta.

Helsingin kaupungin hallintosäännössä on määrätty muun ohella, että kaupunginhallitus huolehtii siitä, että tiedonhallinnan ja asiakirjahallinnon ohjeistus, käytännöt, vastuut ja valvonta on määritelty (24 luku 3 §). Hallintosäännössä määrätään edelleen, että tiedonhallinnan ja asiakirjahallinnon johtaminen kuuluu kaupunginkanslian hallinto-osastolle ja että tietohallinnon ohjaus kuuluu kaupunginkanslian strategiaosastolle.

Tietosuojaa ja asiakirjojen hallintaa koskeva sääntely

Euroopan unionin perusoikeuskirjan 8 artiklassa on turvattu henkilötietojen suoja omana perusoikeutena, kun taas yksityis- ja perhe-elämän suoja on turvattu saman säädöksen 7 artiklassa. Henkilötietoja turvaa myös Euroopan neuvoston ihmisoikeussopimuksen yksityiselämän suojaa koskeva 8 artikla, kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen 17 artiklassa turvattu oikeus yksityis- ja perhe-elämään sekä Suomen perustuslain 10 §:ssä säädetty yksityiselämän suoja ja 22 §:ssä säädetty perus- ja

[51] 731/1999.
[52] 39/1889.
[53] 1050/2018.
[54] HE 9/2018 vp s. 56–56.
[55] 434/2003.
[56] 410/2015.

ihmisoikeuksien turvaamisvelvollisuus. Henkilötietojen suojaa nauttivat myös sellaiset henkilötiedot, jotka eivät kuulu yksityiselämän piiriin.

Tietosuojaa, tietoturvaa sekä henkilötietojen käsittelyä koskevassa lainsäädännössä on tapahtunut paljon muutoksia vuosina 2018–2025.

Euroopan unionin yleisen tietosuoja-asetuksen[57] (GDPR, suomalaisittain lyhennettynä TSA eli tietosuoja-asetus) soveltaminen alkoi 25.5.2018. Asetuksen toimeenpanemiseksi Suomessa tehtiin muutoksia useisiin säädöksiin, joista tärkein oli tietosuojalain säätäminen ja henkilötietolain[58] kumoaminen.

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelystä ja niiden vapaasta liikkuvuudesta. Asetusta sovelletaan 2 artiklan mukaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

Tietosuoja-asetus on valtaosaltaan sellaista pakottavaa sääntelyä, josta ei voida säätää kansallisesti toisin. Tämän vuoksi tietosuojalaista ei saa kattavaa käsitystä tietosuojan sisällöstä. Kansallisessa tietosuojalaissa säädetään vain niistä seikoista, joiden osalta tietosuoja-asetus edellyttää kansallista sääntelyä tai ainakin sallii sen.

Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan ihmiseen (*rekisteröity*) liittyvät tiedot eli suorien tunnistetietojen lisäksi myös sellaiset tiedot, joiden avulla tietty ihminen voidaan esimerkiksi lisätietojen avulla tunnistaa. *Rekisterinpitäjänä* pidetään ihmistä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa *määrittelee* henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjyys saattaa määrittyä myös lainsäädännön kautta.

Helsingin kaupunki on rekisterinpitäjä niiden henkilötietojen osalta, joita se on käsitellyt toimintaansa varten joko määrittelemällä itse käsittelyn tarkoituksen ja keinot tai käsittelemällä henkilötietoja lakisääteisen tehtävänsä toteuttamiseksi. Tietosuoja-asetuksessa asetetaan rekisterinpitäjälle lukuisia käsittelyyn liittyviä velvollisuuksia.

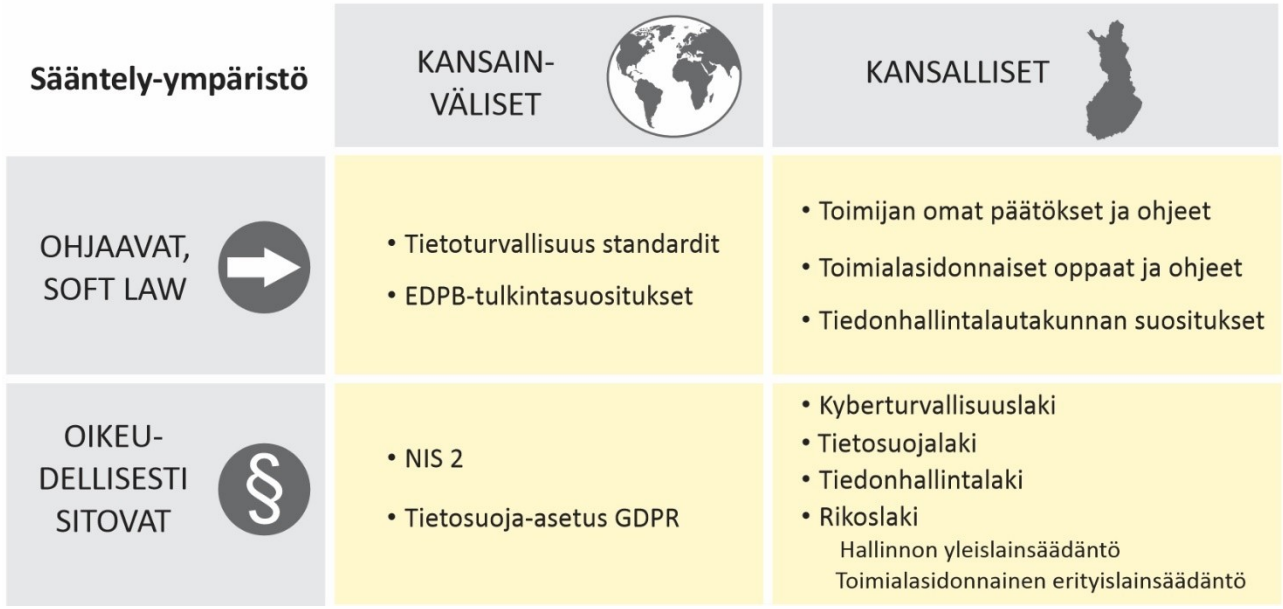
Julkisen hallinnon tiedonhallinnasta annettua lakia[59] (tiedonhallintalaki) sovelletaan myös viranomaisten suorittamaan tiedonhallintaan ja tietojärjestelmien käyttöön. Lain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen, laadukas, turvallinen ja tehokas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi, sekä tietojärjestelmien ja tietovarantojen yhteen toimivuuden edistäminen. Tiedonhallintalain 3 §:n mukaan lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja. Tiedonhallintalain 2 §:ssä määritetään tiedonhallintalaissa käytetyt käsitteet. Tiedonhallintalain 4 §:n 1 momentissa säädetään, että kunnat ja kuntayhtymät ovat lain tarkoittamia tiedonhallintayksiköitä. Ennen tiedonhallintalain voimaantuloa julkisen hallinnon tietoaineistojen käsittelystä ja tiedonhallinnasta ei säädetty yhdellä yleissäädöksellä. Tiedonhallintalain voimaantulon jälkeenkin viranomaisten tiedonhallintaa koskevista velvollisuuksista säädetään myös muissa hallinnon yleissäännöksissä, muun muassa julkisuuslaissa, arkistolaissa sekä tietosuoja-asetuksessa. Säädöksen käyttöönotto on vaatinut huomattavia uudistuksia tiedonhallintayksiköiltä.

[57] (EU) 2016/679.
[58] 524/1999.
[59] 609/2019.

Viranomaisten toiminnan julkisuudesta annetussa laissa (julkisuuslaki)[60] säädetään viranomaisten velvollisuuksista edistää julkisuutta ja avoimuutta sekä oikeudellisista edellytyksistä rajoittaa niitä. Julkisuuslain 24 §:ssä säädetään muun muassa salassa pidettävistä tiedoista. Tiedonhallintalain organisatorinen soveltamisala on säädetty julkisuuslaissa.

Arkistolaissa[61] säädetään arkistonmuodostajan velvollisuuksista. Arkistolain 7 §:n mukaan arkistotoimen tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeeton aineisto. Arkistointia hoidettaessa on tuettava julkisuusperiaatteen toteutumista yksityisten ja yhteisöjen oikeusturva sekä tietosuoja huomioon ottaen. Helsingin kaupunki on osaltaan *arkistonmuodostaja*, jonka arkistotoimen järjestämisestä vastaa arkistolain 9 §:n mukaan kaupunginhallitus.

Hallintolain 7 §:n mukaan viranomaisen on pyrittävä järjestämään asiointi ja asian käsittely siten, että hallinnossa asioiva saa asianmukaisesti hallinnon palveluita ja viranomainen voi suorittaa tehtävänsä tuloksellisesti.



Kuva 13. Tiedonhallinnan, tietoturvan ja tietosuojan sääntely-ympäristö.

Tietosuojaa koskevat vaatimukset

Tietosuoja-asetus asettaa henkilötietojen käsittelylle monenlaisia edellytyksiä ja rekisterinpitäjälle monenlaisia velvollisuuksia. Ensinnäkin käsittelylle tulee aina olla tietosuoja-asetuksessa säädetty peruste. Yleiset perusteet henkilötietojen käsittelylle säädetään TSA 6 artiklassa, jota tietosuojalain 4 § täydentää. Viranomaisten osalta käsittelyn perusteita ovat yleensä rekisterinpitäjän lakisääteisen velvoitteen toteuttaminen, yleistä etua koskevan tehtävän suorittaminen tai julkisen vallan käyttäminen. Myös suostumus, sopimuksen täytäntöönpaneminen ja elintärkeiden etujen suojaaminen ovat mahdollisia käsittelyn perusteita.

[60] 621/1999.
[61] 831/1994.

Erityisiä henkilötietoryhmiä koskevasta käsittelystä säädetään TSA 9 artiklassa. Erityisiä henkilötietoryhmiä ovat esimerkiksi etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus ja terveyttä koskeva tieto. Esimerkiksi koululaisen uskonnollinen vakaumus ja terveystiedot kuuluvat siten erityisten henkilötietojen luokkaan.

Erityisten henkilötietojen käsittely on lähtökohtaisesti kiellettyä, mutta kieltoon on useita poikkeuksia. Käsittely on sallittua esimerkiksi silloin, kun käsittely johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä, jota esimerkiksi varhaiskasvatuksen ja perusopetuksen järjestäminen ovat. Tietosuojalaissa on säädetty erityisten henkilötietojen osalta, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. Näitä ovat esimerkiksi

- toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty
- toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista
- tietosuojavastaavan nimittäminen
- rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin
- henkilötietojen pseudonymisointi
- henkilötietojen salaaminen
- toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi
- erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen
- tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskevan vaikutustenarvioinnin laatiminen
- muut tekniset, menettelylliset ja organisatoriset toimenpiteet.

Rikostuomioihin ja rikoksiin liittyvästä käsittelystä säädetään erikseen TSA 10 artiklassa sekä tietosuojalain 7 §:ssä.

TSA 5 artiklan 1 kappaleessa esitetään henkilötietojen käsittelemistä koskevat periaatteet, joita on noudatettava aina, kun henkilötietoja käsitellään. Saman artiklan 2 kappaleen mukaan rekisterinpitäjä vastaa siitä, että näitä periaatteita on noudatettu ja rekisterinpitäjän tulee myös pystyä *osoittamaan*, että näin on tapahtunut (osoitusvelvollisuus).

Tietosuojaperiaatteiden mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten

- käsiteltävä luottamuksellisesti ja turvallisesti.

Tietosuoja-asetuksen (TSA) 24 artiklassa säädetään siitä, miten rekisterinpitäjän on toimittava varmistaakseen ja osoittaakseen, että henkilötietojen käsittelyssä toimitaan lainmukaisesti. Säännöksen 1. kappaleen mukaan rekisterinpitäjän on toteutettava tarvittavat *tekniset* ja *organisatoriset* toimenpiteet, joilla voidaan *varmistaa* ja *osoittaa*, että käsittelyssä noudatetaan tietosuoja-asetusta. Sitä, millaisia teknisiä ja organisatorisia toimia kulloinkin vaaditaan, arvioidaan ottamalla huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä ihmisten oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Erityisten henkilötietojen osalta edellytetään tarkempia prosesseja ja vankempia turvatoimia kuin sellaisten henkilötietojen osalta, jotka eivät esimerkiksi sisällä rekisteröidyn yksityiselämän piiriin kuuluvia tietoja. Edellytettyihin toimiin vaikuttavat myös esimerkiksi TSA 5 artiklan 1 kohdan mukaiset tietosuojaperiaatteet.

Teknisiin tietoturvatoimenpiteisiin kuuluvat esimerkiksi laitteille ja järjestelmiin pääsyn valvonta, tietojen ja järjestelmien luvattoman käytön estäminen, tapahtumien kirjaaminen, tietoliikenteen alkuperä- ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta. Tarpeen mukaan tietojärjestelmä on suojattava esimerkiksi niin, että jo laittomat yritykset päästä käsiksi henkilötietoihin aiheuttavat hälytyksen rekisterinpitäjälle.

Organisatorisiin toimenpiteisiin kuuluvat esimerkiksi organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyt sekä ohjeistus, koulutus ja valvonta. Rekisterinpitäjän on huolehdittava esimerkiksi siitä, että käyttäjän oikeudet vastaavat hänen asemaansa ja vastuitaan, ja että käyttäjä saa pääsyn vain sellaisiin tietoihin, joiden käsittely on tarpeen hänen työtehtäviensä hoitamiseksi. Henkilötietojen käsittelyoikeuksien tulee olla sitä rajatummat mitä arkaluontoisemmista tai sensitiivisemmistä tiedoista on kyse. Tarpeen mukaan on myös luotava menettelytavat, kuten esimerkiksi lokitietojärjestelmä, joiden avulla voidaan seurata tietojen käyttöä ja tietojen luovuttamista.

Riittävää ei ole se, että tekniset ja organisatoriset toimenpiteet saatetaan kerran kuntoon ja unohdetaan sen jälkeen, vaan toteutettuja toimenpiteitä on tarkasteltava säännöllisesti ja päivitettävä tarvittaessa.

Rekisterinpitäjän *osoitusvelvollisuus* perustuu sekä TSA 5 artiklan 2 kappaleeseen että TSA 24 artiklan 1 kappaleeseen. Ensinnäkin varautuminen osoitusvelvollisuuteen ”pakottaa” rekisterinpitäjän pohtimaan ja kirjaamaan prosessejaan, jolloin saatetaan huomata puutteita, jotka ehditään korjaamaan ennen kuin konkreettista vahinkoa on tapahtunut. Toisekseen rekisterinpitäjä voi osoitusvelvollisuuden avulla näyttää, että se on aktiivisesti pyrkinyt tunnistamaan tietosuojaan liittyviä riskejä ja ottanut käyttöön tarvittavia toimenpiteitä henkilötietojen suojaamiseksi. Osoitusvelvollisuuden toteuttamatta jättäminen on tietosuoja-asetuksen vastaista siinäkin tapauksessa, että mitään muuta konkreettista tietosuojarikettä ei olisi tapahtunut.

Osoitusvelvollisuus tarkoittaa myös *dokumentointivelvollisuutta*, joka käytännössä toteutetaan tiettyjen toimenpiteiden tekemisellä ja kirjaamisella. Osoitusvelvollisuuden laajuus riippuu muun muassa organisaation koosta sekä henkilötietojen määrästä ja laadusta. Osoitusvelvollisuutta voivat osaltaan toteuttaa esimerkiksi seloste käsittelytoimista, tietosuojaa koskevat toimintaperiaatteet sekä sisäiset ja ulkoiset ohjeistukset, informointikäytännöt, käsittelyn oikeusperustetta koskevat arviot, vaikutustenarviointeja ja ennakkokuulemista koskeva dokumentaatio, tietoturvaloukkausten dokumentointi ja niistä seurannut prosessi, tietosuoja-

vastaavan asemaan ja tehtäviin liittyvä dokumentaatio, tietojenkäsittelysopimukset, yhteisrekisterinpitäjien vastuualueiden määrittely sekä henkilötietojen siirtoa kolmansiin maihin koskeva dokumentaatio.

Tietosuoja-asetuksessa on säännöksiä myös henkilötietojen käsittelyn turvallisuudesta. Asetuksen 25 artiklassa säädetään *sisäänrakennetusta ja oletusarvoisesta tietosuoja*sta, jolla pyritään siihen, että tietosuoja otettaisiin huomioon jo tietojärjestelmiä ja henkilötietojen käsittelytoimia suunniteltaessa eikä vasta sitten, kun tietojärjestelmä tai palvelu on jo teknisesti valmis. Tietosuoja- ja tietoturvatoimenpiteiden integroiminen mukaan toimintaan on helpompaa suunnitteluvaiheessa kuin pyrkimällä muokkaamaan valmista järjestelmää tai toimintatapaa jälkikäteen tietoturvallisempaan suuntaan.

Säännöksen mukaan rekisterinpitäjän on – ottaen huomioon uusimman teknologian, toteuttamiskustannukset ja käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit ihmisten oikeuksille ja vapauksille – käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden toteuttamisen edellyttämät tekniset ja organisatoriset toimenpiteet. Tietojen minimointiperiaatteen turvaamiseksi säädetään nimenomaisesti, että rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan se, että oletusarvoisesti käsitellään vain niitä henkilötietoja, jotka ovat käsittelyn tarkoituksen kannalta tarpeellisia. Tämä koskee sekä kerättyjen henkilötietojen määrää että käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Artiklassa todetaan lisäksi, että rekisterinpitäjän on varmistettava etenkin se, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville.

Tietosuoja- ja tietoturvatoimien riittävyyttä on arvioitava jatkuvasti ja niitä on esimerkiksi käsittelytoimien muuttuessa tai teknologian kehittyessä päivitettävä. Rekisterinpitäjän on arvioitava myös käyttämiensä käsittelijöiden toimia ja pyrittävä varmistumaan niiden toimien lainmukaisuudesta.

Tietoturvalla tarkoitetaan tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista siten, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. TSA 32 artiklassa säädetään *käsittelyn turvallisuudesta.* Sen mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.

Arvioitaessa toimenpiteiden asianmukaisuutta on otettava huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Tässä tarkoitettuja toimenpiteitä voivat olla esimerkiksi henkilötietojen pseudonymisointi ja salaus; kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa sekä menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Käytännössä toimenpiteitä voidaan toteuttaa esimerkiksi ottamalla käyttöön pääsynvalvonta laitteille ja järjestelmiin, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperä- ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen sekä tietojen ja

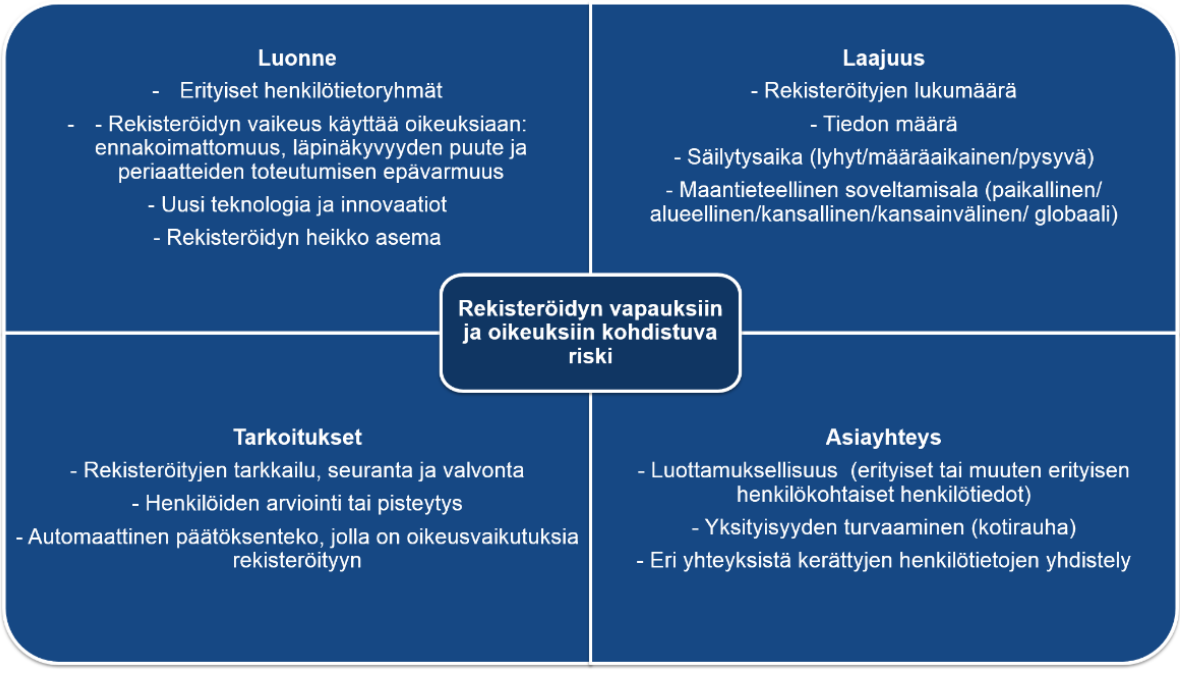
järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten tietojen hakkeroinnilta, viruksilta ja muilta haittaohjelmilta.

Säännöksessä muistutetaan vielä siitä, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen niiden alaisuudessa toimiva ihminen, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei Euroopan unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita. Tämä edellyttää muun muassa henkilökunnan kouluttamista ja ohjeistamista. Ohjeistuksen antaminen puolestaan edellyttää sitä, että rekisterinpitäjä tietää, mitä tietoja sen toiminnassa käsitellään ja miksi, ja että tietosuoja- ja tietoturvanäkökohdat on otettu huomioon käsittelyä järjestettäessä.

Tietosuojaa koskevasta *vaikutustenarvioinnista* säädetään TSA 35 artiklassa. Sen mukaan rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle, jos käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin.

Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Lisäksi se auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, dokumentoinnissa ja osoittamisessa. Arviointi vaaditaan erityisesti muun muassa niissä tapauksissa, joissa laajamittainen käsittely kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin, joita ovat esimerkiksi uskonnollista vakaumusta ja terveydentilaa koskevat tiedot. Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista ja sitä on päivitettävä tarvittaessa

Tietosuojavaltuutettu on kuvannut riskin muodostumista seuraavalla kuvalla (kuva 14):



Kuva 14. Riskin muodostuminen tietojen käsittelyssä. (Kuva: Tietosuojavaltuutetun toimisto)[62]

[62] Tietosuojavaltuutetun toimisto: Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. 26.2.2025 https://tietosuoja.fi/arvioi-riskit

Tietosuoja-asetuksessa säädetään, että rekisterinpitäjän on *ilmoitettava* valvontaviranomaiselle havaitsemastaan *tietoturvaloukkauksesta* 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on paljastunut ja ilmoitettava tapahtuneesta myös rekisteröidyille, jos tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin ihmisten oikeuksille ja vapauksille. Ilmoitusten tarkoituksena on selvittää tietosuojaloukkauksen toteutuminen, mutta myös käynnistää varotoimet, joilla tietojen väärinkäytön mahdollisuuksia pienennetään (33 ja 34 artiklat).

Velvollisuudesta nimittää *tietosuojavastaava* säädetään tietosuoja-asetuksen 37 artiklassa. Mainitun säännöksen perusteella Helsingin kaupungilla on oltava nimettynä tietosuojavastaava.

Tiedonhallintalain asettamat tietoturvallisuusvaatimukset

Tiedonhallintalaki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteen toimivuudesta, tietojärjestelmien yhteen toimivuuden toteuttamisesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.

Säädöksen 13 §:ssä asetetaan viranomaiselle seuraavat tietoturvallisuutta koskevat oikeudelliset vaatimukset:

- Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.
- Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava säännöllisesti riittävällä testauksella.
- Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.
- Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.
- Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

Vaatimukset ovat periaateluontoisia. Ne eivät sisällä yksityiskohtaisia määräyksiä siitä, miten tai millä menetelmillä tietoturvallisuudesta on huolehdittava.

Katakri 2020 -nimistä tietoturvallisuuden auditointityökalua viranomaisille voidaan käyttää apuna arvioitaessa organisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Ensimmäinen Katakri eli kansallinen turvallisuusauditointikriteeristö valmistui jo vuonna 2009. Katakri on jaettu kolmeen osa-alueeseen:

- *Turvallisuusjohtamista* koskevassa osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä 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.

- **Kybermittari** [63] on Kyberturvallisuuskeskuksen kehittämä kansainvälisiin kyberkyvykkyyksien mittausmalleihin pohjautuva mittaristo. Suomessa toimivien yritysten ja organisaatioiden tarpeisiin räätälöity Kybermittari auttaa parantamaan yritysten, organisaatioiden ja samalla koko yhteiskunnan kykyä torjua kyberuhkia. Kybermittari tuo yritysten ja organisaatioiden johdolle ja tietoturva-ammattilaisille konkreettisen työkalun kyberuhkien aiempaa parempaan hallintaan.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö[64] on puolestaan tiedonhallintalautakunnan laatima suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä. Se tukee julkishallinnon tietoturvallisuuden kehittämistä ja arviointia. Sitä voidaan käyttää apuna myös arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Sen tietosuojaa koskeva osa on laadittu yhteistyössä Tietosuojavaltuutetun toimiston kanssa.

ISO/IEC 27001 on tietoturvallisuuden hallintajärjestelmien tunnustetuin kansainvälinen standardi. Siinä määritellään organisaation tietoturvallisuuden hallintajärjestelmän perustamista, täytäntöönpanoa, ylläpitoa, seurantaa ja parantamista koskevat vaatimukset. Se auttaa organisaatioita laatimaan tietoturvan hallintapolitiikan sekä toteuttamaan tarvittavat valvontatoimet ja asettamaan selkeät tavoitteet tietoturvan parantamiseksi.

Tiedonhallintalain 15 §:ssä säädetään tietoaineistojen turvallisuuden varmistamisesta. Tämä käsittää sen, että tietoaineistojen muuttumattomuus on riittävästi varmistettu; tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta; tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu; tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu; tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu; ja tietoaineistot voidaan tarvittavilta osin arkistoida. Laki edellyttää myös, että tietoaineistoja käsitellään ja säilytetään toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.

Tiedonhallintalain 16 § edellyttää, että se viranomainen, joka on vastuussa tietojärjestelmästä, määrittää tietojärjestelmän käyttöoikeudet käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja pitää ne ajantasaisina.

Tiedonhallintalain 17 §:ssä säädetään, että viranomaisen on huolehdittava, että tietojärjestelmien käytöstä kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen keräämisen tarkoituksena on tietojen käytön ja luovutusten seuranta sekä teknisten virheiden selvittäminen.

Tietojen hallinta ja tiedon elinkaari

Tiedonhallintalain 5 §:n mukaan tiedonhallintayksikössä on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa *tiedonhallintamallia*. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteen toimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

---

[63] Kybermittari https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilan-nekuva-ja-verkostojohtaminen/kybermittari

[64] Julkri; Valtiovarainministeriön julkaisuja 2023:46.

Tiedonhallintalain 26 §:n mukaan tiedonhallintayksikön on muodostettava viranomaisen käsiteltäväksi otetun tai annetun asian yksilöivä asiatunnus, jonka avulla asiaan liittyvät tiedot yksilöidään. Säännös liittyy nimenomaisesti hallintoasioiden käsittelyyn, joita tutkittavan tapauksen alalla ovat esimerkiksi henkilöstöä koskeva päätöksenteko, oppilaaksi ottamista koskeva päätöksenteko, oppilaalle annettavaa tukea koskeva päätöksenteko ja maksuvelvollisuutta koskeva päätöksenteko.

Tiedonhallintalain 27 §:ssä säädetään tietoaineistoista, joita muodostuu palvelujen tuottamisen yhteydessä muutoin kuin varsinaisissa asian käsittelyprosesseissa (palvelujen tiedonhallinta). Tämän säännöksen piiriin jäävät kaikki ne muut viranomaisen laatimat tai sille muodostuvat tietoaineistot, joita ei käsitellä loogisessa asiarekisterissä. Tietomurron kohteena ollut aineisto on kuulunut pääosin tämän säännöksen piiriin.

Tiedonhallintayksikön on järjestettävä muun kuin asiankäsittelyn yhteydessä muodostuvan tietoaineiston hallinta siten, että tietoaineistosta muodostettavat asiakirjat ovat haettavissa jollakin tietokokonaisuudet yksilöivällä tunnuksella, jotta tiedot voidaan antaa siihen oikeutetulle vaivattomasti. Viranomaisen on rekisteröitävä palveluja tuotettaessa muodostuvat asiakirjat ja muut tiedot viipymättä siten, että niiden muodostuminen palvelua tuotettaessa voidaan jälkikäteen todentaa. Ennen tiedonhallintalain säätämistä Suomessa ei ollut voimassa vastaavaa säännöstä palvelujen tiedonhallinnasta[65]. Tiedonhallintalautakunta on antanut tarkentavan suosituksen palvelujen tiedonhallinnasta ja sen kehittämisestä (ks. s. 60.)

Tiedonhallintalain 21 §:n mukaan rekisterinpitäjän on määrättävä tietoaineistoille säilytysaika. Säilytysajan päättymisen jälkeen tiedot on tuhottava. Ne tiedot, jotka on laissa säädetty arkistoivaksi tai muilla perusteilla niitä katsotaan olevan tarpeen säilyttää, arkistoidaan arkistolain mukaan.

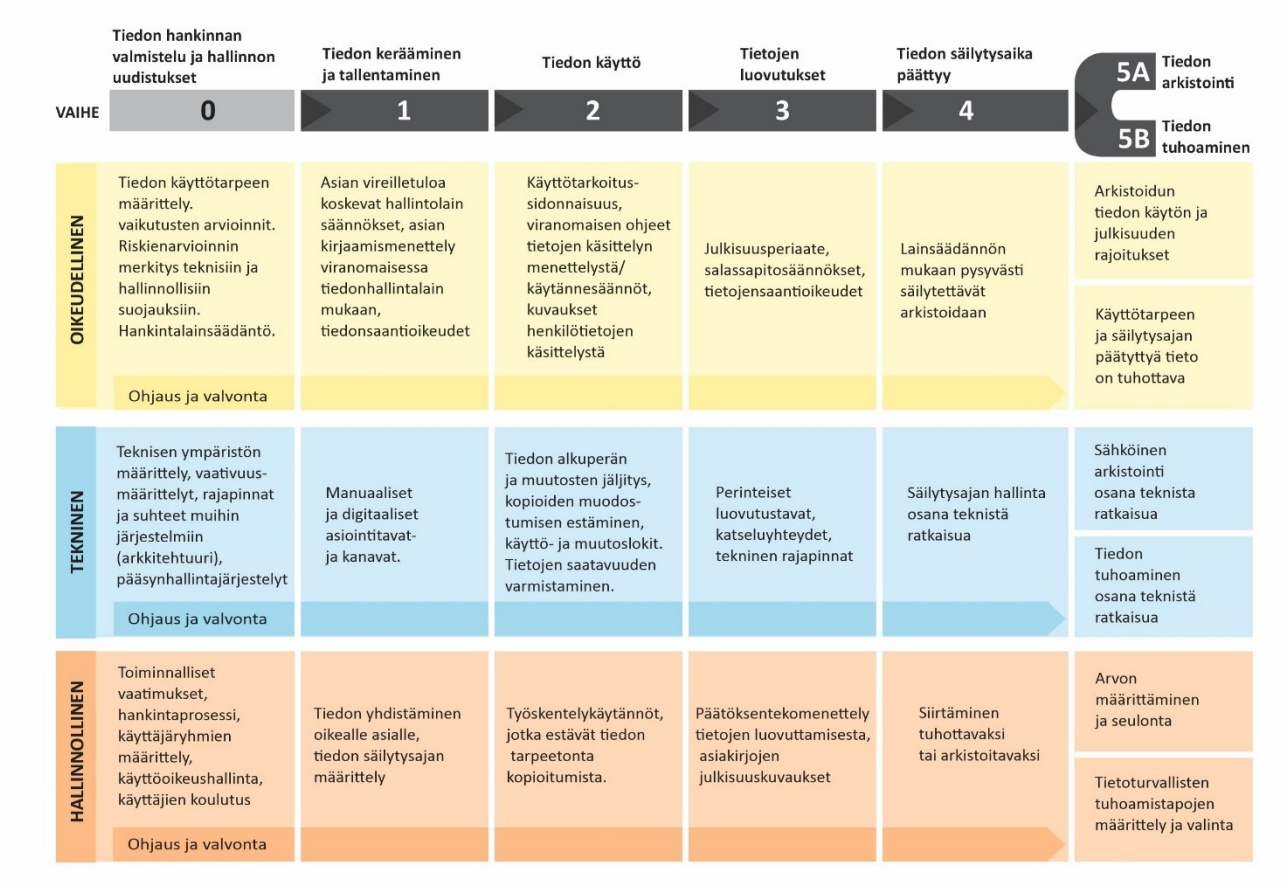
Koulutuksen henkilörekistereiden nimistä tai sisällöistä ei ole nimenomaisesti säädetty, pois lukien opiskeluhuoltorekisteri, josta on säädetty oppilas- ja opiskelijahuoltolaissa[66]. Koulutuksen tietojenkäsittelyssä noudatetaan siten pitkälti tiedonhallinnan, tietosuojan sekä julkisuuden yleissääntelyä.

Arkistolain mukaan arkistotoimen tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeeton aineisto. Arkistonmuodostamista varten ylläpidetään tiedonohjaussuunnitelmaa (nk. TOS). Tiedonohjaussuunnitelma tiedonhallintamalliin kytkeytyvät suunnittelukokonaisuus.

Tietojen hävittäminen tulee toteuttaa sen jälkeen, kun tiedolle määrätty säilytysaika on päättynyt tai tiedon käyttötarve on muutoin loppunut. Yleiset ohjeet tietojen säilyttämisajoista perustuvat muun muassa säilytysaikaohjeisiin.[67]

---

[65] HE 248/2028 vp. Hallituksen esitys Eduskunnalle tiedonhallintalaiksi.
[66] 1287/2013.
[67] Kunnallisten asiakirjojen säilytysajat. Määräykset ja suositukset. Opetustoimi 12. 25.2.2025 https://www.kuntaliitto.fi/julkaisut/2002/1349-kunnallisten-asiakirjojen-sailytysajat-maaraykset-ja-suositukset-opetustoimi-12



Kuva 15. Tiedon elinkaaren oikeudellisia, hallinnollisia ja teknisiä näkökulmia.

Tietojen julkisuus ja salassapito

Julkisuuslaissa säädetään tietojen julkisuudesta ja salassapidosta. Julkisuuslain lähtökohtana on tietojen julkisuus ja viranomaisen velvollisuus edistää julkisuutta. Julkisuuslain 24 §:ssä säädetään niistä tietoryhmistä, joita koskevat asiat ovat salassa pidettäviä ja oikeus näiden tietojen saantiin on rajoitettua.

Julkisuuslain 24 §:n 1 momentin 30 kohdan mukaan salassa pidettäviä asioita ovat muun muassa;

- oppilashuoltoa ja oppilaan opetuksesta vapauttamista koskevat asiakirjat,
- oppilaan ja kokelaan koesuoritukset sekä
- sellaiset oppilaitoksen antamat todistukset ja muut asiakirjat, jotka sisältävät oppilaan henkilökohtaisten ominaisuuksien sanallista arviointia koskevia tietoja,
- samoin kuin asiakirjat, joista ilmenee ylioppilastutkintolautakunnan määräämien arvostelijoiden arvostelutehtäviä koskeva koulukohtainen työnjako, kunnes on kulunut vuosi kyseisestä tutkintakerrasta.

Saman momentin 32 kohdan mukaan salassa pidettäviä ovat myös muun muassa asiakirjat, jotka sisältävät tietoja henkilön yksityiselämän piirissä esittämistä mielipiteistä taikka tietoja henkilön elintavoista, osallistumisesta yhdistystoimintaan tai vapaa-ajan harrastuksista, perhe-elämästä tai muista niihin verrattavista henkilökohtaisista oloista.

Opetustoimessa on erityislainsäädännössä joitakin määräyksiä salassa pidettävistä tiedoista koskien oppilas- ja opiskelijahuoltoa sekä koulun henkilökunnan välistä tietojen vaihtoa.[68]

Tietomurron uhrin asema, tietojen suojaaminen ja vahinkojen korvaaminen

Tietomurron uhrilla on tietosuoja-asetuksen 82 artiklan perusteella oikeus saada *rekisterinpitäjältä tai henkilötietojen käsittelijältä* korvausta tietosuoja-asetuksen rikkomisesta aiheutuneesta vahingosta. Korvausvastuun edellytyksenä on, että 1) vahinkoa on aiheutunut joko rekisteröidylle tai muulle henkilölle; 2) henkilötietojen käsittely on ollut tietosuoja-asetuksen vastaista ja 3) tietosuoja-asetuksen vastaisen henkilötietojen käsittelyn ja vahingon välillä on syy-yhteys. Korvausvastuun peruste määräytyy tietosuoja-asetuksen 82 artiklan perusteella, kun taas korvauksen määrän arviointiin sovelletaan kansallista lakia; tavallisesti vahingonkorvauslakia.[69] Kysymys voi olla esimerkiksi tilanteesta, jossa rekisterinpitäjä on suojannut rekisterin niin huonosti, että tietomurron tekeminen on mahdollistunut.

Jos kysymys on muun kuin rekisterinpitäjän tai tietojen käsittelijän aiheuttamasta vahingosta, vahingonkorvausta voidaan vaatia vahingonkorvauslain perusteella. Puhdas varallisuusvahinko eli taloudellinen vahinko, joka ei ole yhteydessä henkilö- tai esinevahinkoon, korvataan vahingonkorvauslain 5 luvun 1 §:n mukaan, kun se on aiheutettu rangaistavaksi säädetyllä teolla tai julkista valtaa käytettäessä taikka milloin muissa tapauksissa on erittäin painavia syitä. Kärsimys puolestaan korvataan vahingonkorvauslain 5 luvun 6 §:n mukaan muun muassa silloin, kun se on aiheutettu vapautta, rauhaa, kunniaa tai yksityiselämää loukkaavalla rangaistavaksi säädetyllä teolla. Jos tietomurrosta seuraa henkilövahinko, sekä korvataan tuottamuksen perusteella vahingonkorvauslain 5 luvun 2 §:n mukaisesti.

Korvattavaa aineellista vahinkoa ovat esimerkiksi tietomurrosta mahdollisesti aiheutunut ansionmenetys ja luottokiellon hankkimisesta aiheutuneet kulut. Aineetonta vahinkoa ovat esimerkiksi henkinen kärsimys sekä tilapäisenä haittana ilmenevä akuutti stressireaktio. Tietomurrosta voi joissakin tapauksissa seurata myös henkilövahingoksi luokiteltava psyykkinen sairaus, kuten esimerkiksi masennus tai paniikkihäiriö. Tällöin korvataan esimerkiksi sairaanhoitokulut, ansionmenetys sekä sairauden aiheuttama kärsimys ja/tai pysyvä taikka tilapäinen haitta.

Euroopan unionin tuomioistuin on katsonut, että myös pelko henkilötietojen mahdollisesta tulevasta väärinkäytöstä on tietosuoja-asetuksen 82 artiklan nojalla korvattavaa vahinkoa, kunhan pelko ei ole täysin hypoteettinen.[70] *Tapauksessa VB v. Natsionalna agentsia za prihodite*[71] EUT totesi, että tietosuoja-asetuksessa ei erotella tilanteita sen suhteen, aiheutuuko sen rikkomisesta kärsimystä sen vuoksi, että asianomaisen henkilötietoja on käytetty väärin jo korvausvaatimuksen esittämisajankohtana, vai sen vuoksi, että asianomainen pelkää tulevaisuudessa tapahtuvaa väärinkäyttöä. Asetuksen sanamuoto ei sulje pois sitä vaihtoehtoa, että ilmaisu ”aineeton vahinko” muodostuu pelosta, että kolmannet osapuolet käyttävät henkilötietoja asetuksen rikkomisen seurauksena väärin. Vahingonkärsijän on kuitenkin osoitettava pelosta aiheutuneen kielteisiä seurauksia. Tietomurron uhrille voi aiheutua merkittävää kärsimystä sen vuoksi, että hän pelkää tietojen tulevan myöhemmin esiin jossakin yllättävässä yhteydessä jopa julkisesti esimerkiksi internetsivustolla.

---

[68] Säännökset ovat muun muassa perusopetuslain (628/1998) 40 §, lukiolain (629/1998) 32 §, ammatillisesta koulutuksesta annetun lain (531/2017) 109 §.
[69] 412/1974.
[70] Esimerkiksi Österreichische Post, C-300/21 ja GP v. juris GmbH, C-741/21.
[71] C-340/21.

Tietomurtovahinkojen erityispiirre on, ettei vahinkotilannetta saada vahingonkorvauksella ennallistettua vahinkoa edeltänyttä tilannetta vastaavaksi, koska tietojen myöhempi väärinkäyttö on mahdollista.

Valtiokonttori voi rikosvahinkolain nojalla maksaa henkilövahingosta aiheutuneita kuluja sekä korvausta kivusta ja särystä sekä tilapäisestä ja pysyvästä haitasta. Kärsimys korvataan valtion varoista vain tietyissä vakavissa tapauksissa, minkä vuoksi kärsimyskorvausta ei voida myöntää tietomurron tai yksityiselämää loukkaavan tiedon levittämisen perusteella. Kärsimyskorvausta voidaan myöntää kiristyksen tai sen yrityksen perusteella. Yleisesti ottaen rikosvahinkolaissa määritelty korvaussuoja on suppeampi kuin vahingonkorvauslaissa säädetty korvausoikeus, mutta se antaa uhrille tiettyä minimiturvaa, josta on hyötyä rikoksentekijän maksukyvyttömyystilanteissa.

Rikos- ja korvausoikeudenkäynteihin liittyvän oikeudenkäyntikuluriskin lisäksi on otettava huomioon myös se, että oikeudenkäynnit ja niihin liittyvät aineistot ovat lähtökohtaisesti julkisia. Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa[72] mahdollistaa esimerkiksi asianomistajan henkilöllisyyden salassapidon rikosasiassa, joka koskee erityisen arkaluonteista hänen yksityiselämäänsä liittyvää seikkaa sekä yksityiselämään tai terveydentilaan liittyviä arkaluonteisia tietoja sisältävän asiakirjan salassapidon. Tästä huolimatta tietoja saattaa vuotaa tai kaikkia asianosaisen salassa pidettäväksi esittämiä tietoja ei määrätä salassa pidettäviksi. Tämän takia asian saaman lisäjulkisuuden pelko voi joissakin tapauksessa johtaa siihen, että tietomurron uhri ei halua vaatia rangaistusta tai vahingonkorvausta, johon hänellä olisi oikeus.

Henkilötunnus (HETU) on pysyväksi tarkoitettu ihmisen yksilöimiskeino. Tietomurron uhrit pelkäävät usein sitä, että heidän henkilötunnustaan käytetään esimerkiksi identiteettivarkauden tai petoksen tekemisessä. Pelko on ymmärrettävä, vaikka henkilötunnusta ei sinällään tulisi käyttää tunnistamisen vaan ainoastaan henkilön identifioinnin välineenä – eihän henkilötunnuksen ilmoittaminen ole tae siitä, että kyseessä on henkilötunnuksen tarkoittama henkilö.

Väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain[73] mukaan henkilötunnus voidaan muuttaa vain tiukoin edellytyksin, jotka täyttyvät, jos

- ihmisen syntymäaika tai sukupuoli on merkitty tunnukseen väärin
- ihminen vahvistaa sukupuolensa toiseksi
- joku toinen on käyttänyt ihmisen henkilötunnusta toistuvasti väärin, ja siitä on aiheutunut suurta taloudellista tai muuta haittaa tai
- ihmisen terveyteen tai turvallisuuteen kohdistuu ilmeinen ja pysyvä uhka.

Vastaamon tietomurron (2020) jälkeen selvitettiin henkilötunnuksen muuttamista koskevan sääntelyn muutostarvetta, koska henkilötunnuksia ei voitu muuttaa tietoturvaloukkausten tai tietomurtojen jälkeen ennakollisesti yksilöiden suojaamiseksi. Asiassa päädyttiin kuitenkin siihen, että henkilötunnuksen muuttamisedellytyksiä ei ollut syytä lieventää. Henkilötunnuksen muuttaminen aiheuttaisi ihmiselle monenlaista vaivaa ja kustannuksia asiakirjojen, asiakastietojen ja rekisterien muutos- ja päivitystarpeiden vuoksi.

---

[72] 370/2007.
[73] 661/2009.

Henkilötunnuksen väärinkäyttämistä tunnistamisen välineenä voidaan ehkäistä muun muassa lisäämällä eri tahojen tietoisuutta siitä, että henkilötunnusta ei tule yksin käyttää tunnistamisen välineenä sekä ohjaamalla toimijat käyttämään vahvaa tunnistautumista, kuten mobiilivarmennetta tai pankkitunnuksia. Tietosuojalain 29 §:ssä on säädetty henkilötunnuksen käytöstä tunnistamisessa seuraavasti: ”rekisteröidyn henkilöllisyyden selvittämiseen hänen ilmoittamiensa tai toimittamiensa tietojen taikka esittämiensä asiakirjojen avulla (*tunnistaminen*) ei saa käyttää yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää”.

Informointivelvollisuus ja viranomaisen tiedottamisvelvollisuudet tietomurron uhreille

Tietosuoja-asetuksen 34 artiklan perusteella rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröidylle, mikäli tämän tiedot ovat joutuneet tietoturvaloukkauksen - kuten tietomurron - kohteeksi, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin ihmisen oikeuksille ja vapauksille. Ilmoitus on tehtävä ensisijaisesti henkilökohtaisesti ja ilman aiheetonta viivytystä.

Ilmoituksessa on selkeästi kerrottava, mitä tietoja tietoturvaloukkaus koskee. Lisäksi siinä tulee antaa tiedot tahosta, jolta voi saada lisätietoa, sekä kuvata loukkauksen mahdollisia seurauksia. Rekisterinpitäjän on myös esitettävä toimenpiteet, joilla tietoturvaloukkauksen vaikutuksia on pyritty pienentämään tai voidaan vielä vähentää. Ilmoitusvelvollisuuden tavoitteena on varmistaa, että loukkauksen kohteeksi joutuneet saavat tarvittavat tiedot henkilötietojensa suojaamiseksi ja asianmukaisten toimenpiteiden toteuttamiseksi.

Tilanteissa, joissa rekisteröityjen tavoittaminen vaatisi kohtuutonta vaivaa, voidaan tiedottaminen toteuttaa myös yleisenä tiedoksiantona. Tällöinkin viestinnän on oltava yhtä tehokasta, kattavaa ja saavutettavaa kuin henkilökohtaisessa tiedoksiannossa.[74]

Viranomaisen tiedottamisvelvollisuus ei kuitenkaan rajoitu pelkästään tietosuoja-asetuksen informointivelvollisuuteen. Tiedottamisvelvollisuus on ymmärrettävä tätä laajempana, perustuslain 22.1 §:ssä säädettyyn perusoikeuksien turvaamisvelvollisuuteen liittyvänä tehtävänä. Tehtävä sisältää viranomaiselle kuuluvan velvollisuuden oma-aloitteisesti tiedottaa asioista, jotka ovat laaja-alaisia tai merkittäviä.[75] Mainitun velvollisuuden toteuttamista on valtioneuvoston oikeuskansleri arvioinut muun muassa Korona-viruspandemian poikkeusolotoimivaltuuksien käyttöönottomenettelyyn liittyen. Oikeuskansleri kiinnitti huomioita siihen, että erityisesti poikkeuksellisessa kriisitilanteessa selkeällä ja informatiivisella tiedottamisella on olennainen merkitys ja että viranomaisella on erityinen velvollisuus huolehtia kansalaisten tiedonsaannista.

Tiedottamisen merkitystä korostaa se, että nopeasti syntyneessä tilanteessa viranomaisten tiedotteet voivat olla kansalaisten ainoa informaation lähde. Tällöin tiedottamisessa käytettävien asianmukaisten ja oikeudellisesti täsmällisten ilmaisujen merkitys on olennainen.[76]

Tiedottamisvelvollisuus on säädetty julkisuuslain[77] 20.2 §:ssä, jonka mukaan viranomaisen on tiedotettava toiminnastaan ja palveluistaan sekä yksilöiden ja yhteisöjen oikeuksista ja velvollisuuksista toimialaansa liittyvissä asioissa. Tiedottamisvelvollisuuteen liittyy myös hallintolain 9 §:ssä on säädetty hyvän kielen käytön vaatimus, jonka mukaan viranomaisen on

[74] TSA 34 artikla kohta 1c.
[75] Hallituksen esitys Suomen perustuslaiksi 309/1993 vp, s. 58.
[76] OKV/740/70/2021 ja OKV/61/10/2020.
[77] 621/1999.

käytettävä asiallista ja ymmärrettävää kieltä. Edelleen kielilain[78] 23 §:ssä turvataan kielelliset oikeudet viranomaisten viestinnässä.

Rangaistussäännökset

Rikoslain 38. luvussa on rikostunnusmerkistöt muun muassa tietojärjestelmän häirinnästä (7 a §) ja törkeästä tietojärjestelmän häirinnästä (7 b §), tietomurrosta (8 §) ja törkeästä tietomurrosta (8 a §), suojauksen purkujärjestelmärikoksesta (8 b §) sekä tietosuojarikoksesta (9 §). Syyttäjä ei saa nostaa syytettä tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmärikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikoksentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista (10 § 3 mom.). Syyttäjän on ennen henkilörekisteriin kohdistuvaa tietomurtoa, törkeää tietomurtoa tai tietosuojarikosta koskevan syytteen nostamista kuultava tietosuojavaltuutettua. Tuomioistuimen on tällaista rikosta koskevaa asiaa käsitellessään varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi (30 § 4 mom.). Myös oikeushenkilön rangaistusvastuu voi tulla kysymykseen tietomurron, törkeän tietomurron, tietojärjestelmän häirinnän ja törkeän tietojärjestelmän häirinnän osalta.

Viranomaisten yhteistyöhön tietomurroissa tai kyberturvallisuustapahtumissa ei ole lainsäädännössä määrätty johtavaa viranomaista samalla tavoin kuin tavanomaisiin onnettomuus- tai rikostapahtumiin, joissa yleisjohtovastuu jakautuu tyypillisesti pelastus- tai poliisiviranomaiselle. Kyberturvallisuuteen ja tietoturvaloukkausten ja uhkien selvittämiseen liittyvät viranomaisvastuut on Suomessa hajautettu eri viranomaisten kesken. Jokaisella viranomaisella on oma roolinsa kyberympäristössä tapahtuvien häiriöiden selvittämisessä.

Valtioneuvosto teki 10.6.2021 periaatepäätöksen Vastaamon tietomurron jälkeen tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla. Vastaamon potilastietojärjestelmään murtauduttiin vuosina 2018–2019 ja murto tuli julkisuuteen 21.10.2020, kun tekijä alkoi kiristää ensin yritystä ja sen epäonnistuttua suoraan keskuksen asiakkaita.

Tietomurrossa varastettiin arviolta 33 000 psykoterapiakeskuksen asiakkaan henkilö- ja terveystiedot. Periaatepäätös perustuu liikenne- ja viestintäministeriön johtamana toimineen poikkihallinnollisen työryhmän muistioon ja se tehtiin pääministeri Marinin hallituksen toimintakauden aikana.[79] Periaatepäätöksessä on määritelty 37 yhteiskunnallisen tason toimenpidettä tietosuojan ja tietoturvan parantamiseksi sekä tietomurtotapausten torjumiseksi ja selvittämiseksi yhteiskunnan kriittisillä toimialoilla. Näistä toimenpiteistä noin kolmasosaan on arvioitu kuuluvaksi lainsäädäntömuutoksia.

Periaatepäätöksen edistämis- ja seurantatehtävä kuuluu liikenne- ja viestintäministeriölle. Päätöksessä ei selkeästi määritellä, mitä yhteiskunnan kriittiset toimialat ovat, mutta toimeenpanotoimia käsittelevässä kohdassa annetaan ymmärtää, että kyse olisi NIS-direktiivissä määritellyistä toimialoista. Opetustoimi ei kuulu näihin.

Periaatepäätöksen keskeisiä kehittämiskohteita ovat muun muassa viranomaisten välisen yhteistyön, tietojen vaihdon ja virka-avun parantaminen, tietoturvallisuuden kartoituspalvelun (Hyöky) ja tietomurtojen havaitsemiseen tähtäävä palvelun (Havaro) mahdollistaminen kaikille kriittisille toimialoille, kaikkia toimialoja koskevien lakisääteisten

[78] 423/2003.

[79] Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. 1.3.2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

tietoturvavaatimusten antaminen, kriittisten toimintojen säännönmukainen tietoturvan auditointivelvollisuus sekä tietoturvaloukkausten asiointi- ja viestintäpalvelun perustaminen.

Periaatepäätöksen valmisteluvaiheessa Helsingin kaupunginkanslia antoi 7.4.2021 lausunnon, jossa todetaan, että ”suurilla organisaatioilla, kuten suurimmilla kaupungeilla, on mahdollisuus hankkia riittävää asiantuntijuutta kaikille tarvittaville digitaalisen turvallisuuden osa-alueille, kuten tietosuoja ja kyberturva. Tärkeä asia on, että Suomen 15 suurimman kunnan tietoturvan ja tietosuojan tason selvityksessä hyödynnetään Kyberturvallisuuskeskuksen tarjoamaan tietoturvallisuuden kartoituspalvelua.”

Valtioneuvoston periaatepäätökset ovat luonteeltaan poliittisia linjausasiakirjoja, joilla ei ole välitöntä oikeudellista ohjausvaikutusta. Periaatepäätökset kuitenkin kuvaavat asioita, joiden on tunnistettu vaativan valtioneuvostolta toimenpiteitä. Valtioneuvoston periaatepäätökset ovat hallituskohtaisia. Hallituksen vaihtuessa uusi hallitus on tehnyt erikseen päätöksen siitä mihin periaatepäätöksiin se toiminnassaan sitoutuu. Pääministeri Orpon hallitus on tehnyt mainitun päätöksen 21.3.2024.[80] Tietosuojan ja tietoturvan parantamiseen tähtäävä periaatepäätös on otettu osaksi myös Orpon hallituksen toimintaa ohjaavaksi ja linjaavaksi.

Samassa yhteydessä periaatepäätösten ohjausvaikutusta on katsottu heikentävän niiden suuri määrä, epäyhtenäinen laadintatapa sekä mahdollinen irrallisuus hallitusohjelman kirjauksista.

Periaatepäätöksen seurantatehtävä on kuulunut liikenne- ja viestintäministeriölle, joka on koonnut vastuutahojen tekemien ilmoitusten perusteella yhteenvetoja asiaa seuranneelle ministeriryhmälle.

Periaatepäätöksen lainsäädäntötoimien eteneminen on ollut hidasta tai sääntelyratkaisut ovat muuttuneet periaatepäätöksen laatimisen jälkeen. Merkittäviä muutoksia alan sääntelyyn on tullut kyberturvallisuuslaissa, joka on astunut voimaan 8.4.2025. Sääntelyratkaisuihin ja säännösten sisältöihin on vaikuttanut osaltaan esimerkiksi verkko- ja tietoturvadirektiivin NIS2 kansallinen täytäntöönpano, joka on osa Kyberturvallisuuslain toimeenpanoa.

Periaatepäätökseen sisältynyt ehdotus siitä, että tietomurtotapauksissa viranomaisten yhteistoimintaa tehostettaisiin samoin periaattein kuin muissa vakavissa onnettomuuksissa tai häiriötilanteissa, ei ole ainakaan välittömästi käy ilmi vireillä olevista säädöshankkeista. Tämän toimenpiteen kehittämiseksi annettu hallituksen esitys raukesi valtiopäivien päättyessä 4.4.2023.[81]

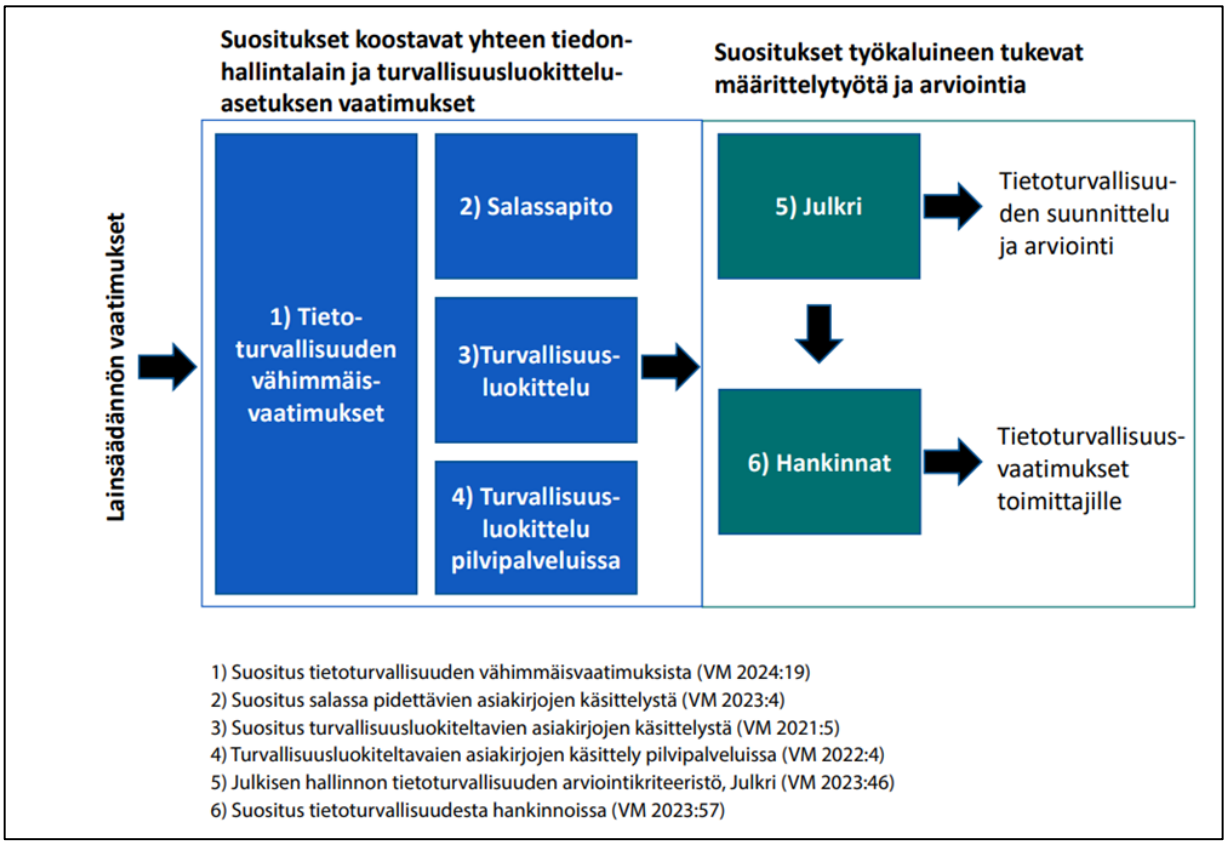
Julkisen hallinnon tiedonhallintalautakunta on antanut kuusi suositusta julkisen hallinnon tietoturvan parantamiseksi. Lisäksi useissa muissa suosituksissa on tietoturvallisuusnäkökulmia. Suositus tietoturvallisuuden vähimmäisvaatimuksista on annettu 11.3.2024. Suositus on kattava ja siinä esitetään perusteet tiedonhallintalain tietoturvallisuusvaatimusten vähimmäissisällöistä julkiseen hallintoon. Tietoturvallisuutta koskevia suosituksia ja parhaita käytäntöjä jakavat myös useat muut toimijat, joiden takia eheä kuva suositeltavista ratkaisuista pilkkoutuu.

Suositus ja kriteeristö tietoturvallisuuden arvioinnin tueksi julkisesta hallinnosta on annettu 12.6.2023. Suositus on yhteensovitettu Tietoturvallisuuden auditointityökalu viranomaisille (Katakri) ja Pilvipalveluiden turvallisuuden arviointikriteeristö (Pitukri) kanssa.

---

[80] VNK: Erillisten valtioneuvoston yleisistunnossa päätettyjen ohjausasiakirjojen voimassaolosta päättäminen. 26.2.2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=1079

[81] HE 243/2022. 25.2.2025 https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_243+2022.aspx



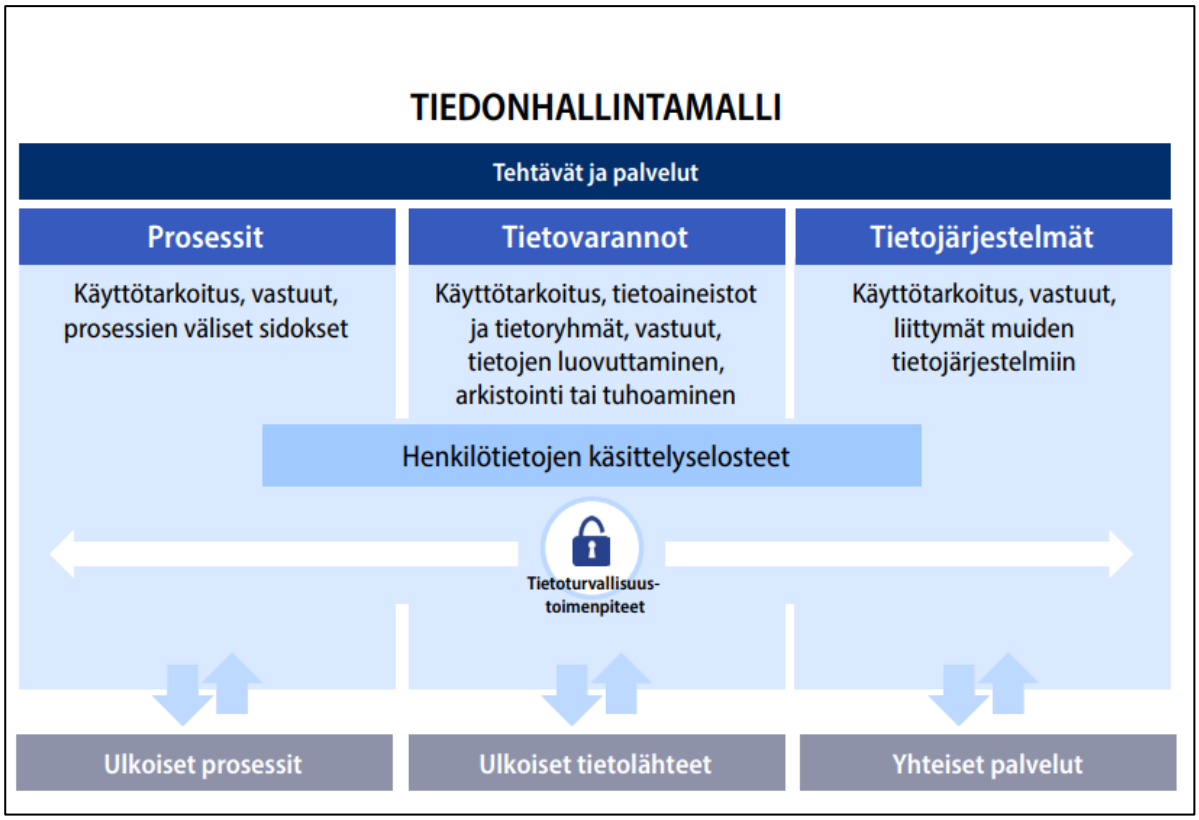
Kuva 16. Tietoturvallisuutta koskevat tiedonhallintalautakunnan suositukset (KUVA: Valtiovarainministeriö 2024)[82]

Tiedonhallintalautakunta on julkaissut suosituksen tiedonhallintamallista. Suosituksella on pyritty selventämään tiedonhallintalain säännöksiä tiedonhallintamallin sisällöstä.

Suosituksen mukaan tiedonhallintamalli on tiedonhallintayksikön työväline ymmärtää ja hallita toimintaympäristöään sekä varmistaa tiedonhallintaa koskevien vaatimusten toteuttaminen. Tiedonhallintamallissa esitetyt tiedot muodostavat perustan, kun tiedonhallintayksikön asiakkaille tuotetaan tiedonhallintalain 28 §:ssä säädetty asiakirjajulkisuuskuvaus.

Suosituksen mukaan tiedonhallintamalli voi tarjota perustiedon organisaation tiedonhallinnan nykytilasta sekä niistä ratkaisuista, joilla se tiedonhallintaansa toteuttaa. Kun tiedonhallintamalli yhdistetään tai linkitetään tiedonhallintayksikössä oleviin erillisiin tiedonhallinnan ohjausmenetelmiin (esimerkiksi arkistonmuodostus, tiedonohjaus, laadunhallinta) voidaan mallia hyödyntää myös tiedon elinkaaren hallinnassa. Tiedonhallintamallissa kuvattavat tietovarantojen tietoaineistojen säilytysajat sekä tieto tietojen arkistoinnista ja tuhoamisesta muodostavat kokonaiskuvan tiedonhallintayksikössä hallittavan tiedon elinkaareen. Vastaavasti tiedonhallintamallissa esitettäviin toimintaprosesseihin voidaan linkittää prosessin eri vaiheissa tietojen käsittelyä ohjaavat metatiedot.

82 Suositus tietoturvallisuuden vähimmäisvaatimuksista, sivu 10. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165487/VM_2024_19.pdf



Kuva 17. Tiedonhallintamallin sisältö.[83] (Kuva: Valtiovarainministeriö 2024)

Tiedonhallintalautakunta on julkaissut suosituksen, joka koskee tiedonhallintaa palvelujen tuottamisen yhteydessä. Suositus käsittelee sitä viranomaisen tietoaineistoa, joka ei sisälly varsinaiseen asiankäsittelyyn. Suositus tukee tiedonhallintalain 27 §:ssä säädetyn velvollisuuden toimeenpanoa. Suosituksessa on kuvattu keinot, joilla tietojen yksilöintiin ja elinkaaren hallintaan liittyvät toimia voidaan toteuttaa.[84]

Tietosuojavaltuutetun ja muiden lainkäyttäjien ratkaisuja julkaistaan Finlex-palvelussa. Ratkaisut muodostavat tapausaineiston, jonka sisältämiä oikeusohjeita voi käyttää tietosuojaa koskevien kysymysten ratkaisemisessa.

Osana tehtävänsä hoitamista tietosuojavaltuutettu tukee tietosuojavelvoitteiden toteuttamista julkaisemalla erilaisia oppaita keskeisistä tietosuojakysymyksistä. Opetuksen ja koulutuksen alalle on muun muassa laadittu opas oppilaan tietojen vaihtamisesta kodin ja koulun välillä.[85] Monet tietosuojavaltuutetun toimiston oppaat on laadittu ennen tietosuoja-asetuksen voimaantuloa, eikä niiden sisältöjen vastaavuutta tietosuoja-asetukseen ole päivitetty. Tämä heikentää oppaiden käytettävyyttä.

[83] Suositus tiedonhallintamallista, sivu 10. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165497/VM_2024_22.pdf

[84] Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa 16.3.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164194/VM_2022_42.pdf?sequence=1&isAllowed=y

[85] Tietosuojavaltuutetun toimisto: Oppilaiden henkilötietojen käsittely kodin ja koulun yhteistyössä. 26.2.2025 https://tietosuoja.fi/documents/6927448/10594424/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4/5169bbf4-c5de-d073-c247-a10a462ca5fb/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4.pdf

Suurin osa koulutus- ja opetustoimen tietosuojaa koskevista oppaista on Opetushallituksen julkaisuja. Oppaat on laadittu yhteistyössä tietosuojavaltuutetun kanssa.

Apulaistietosuojavaltuutettu on vuonna 2021 tehnyt Opetushallitukselle aloitteen opetuksessa käytettävien sovellusten henkilötietojen käsittelystä.[86] Asiaan ei ole kuitenkaan valmistunut valtakunnallista ohjeistusta.

Suomen kyberturvallisuusstrategia[87] vuosille 2024–2035 julkaistiin lokakuussa 2024. Strategia on päivitetty vastaamaan muuttunutta toimintaympäristöä sekä vahvistamaan kyberturvallisuuden asemaa osana kokonaisturvallisuutta. Strategia perustuu neljään keskeiseen pilariin:

1. Osaaminen, teknologia ja tutkimus-, kehitys- ja innovaatiotoiminta (TKI): Tavoitteena on vahvistaa kyberturvallisuusosaamista kaikilla yhteiskunnan tasoilla, edistää innovatiivista kyberekosysteemiä sekä hyödyntää uusia teknologioita, kuten tekoälyä ja kvanttiteknologiaa.
2. Varautuminen: Strategia korostaa ennakoivaa toimintaa kyberuhkien torjumiseksi ja niihin reagoimiseksi, erityisesti kriittisen infrastruktuurin suojaamiseksi ja yhteiskunnan toimintavarmuuden turvaamiseksi.
3. Yhteistoiminta: Tässä painotetaan kansallisen ja kansainvälisen yhteistyön merkitystä, mukaan lukien tiivis yhteistyö EU:n ja Naton kanssa, sekä julkisen ja yksityisen sektorin välistä kumppanuutta kyberuhkien torjunnassa.
4. Reagointi ja vastatoimet: Strategia kehittää valmiuksia nopeaan reagointiin kyberhyökkäyksissä, mukaan lukien kyberpuolustuskyvyn vahvistaminen ja kyberrikollisuuden torjunta.

Strategian tavoitteena on, että Suomi on vuoteen 2035 mennessä kyberturvallisuuden edelläkävijä, jossa digitaalinen ympäristö on turvallinen ja luotettava kaikille käyttäjille. Strategia päivitetään viiden vuoden välein. Sen toimeenpanosuunnitelmaa seurataan ja arvioidaan säännöllisesti.

Kyberturvallisuusstrategian toimeenpanosuunnitelma julkaistiin 4.12.2024.[88] Se koostuu strategian neljän peruspilarin alaisuuteen laadituista 44 kehittämistoimenpiteestä, joista jokaiselle on asetettu tavoite, aikataulu ja rahoitus, vaikutusarvio ja vaikuttavuusanalyysi sekä vastaava(t) organisaatio(t) ja toimija(t).

Digi- ja väestötietovirasto (DVV) lakisääteisenä tehtävänä on tuottaa tiedonhallintalautakunnalle asiantuntijapalveluja[89] tiedonhallinnan ja tietoturvallisuuden menettelyjen kehittämiseksi. Keskeisenä tehtävänä on osallistua lautakunnan jaostojen työhön ja suositusvalmisteluun sekä tukea lautakunnan tehtävien hoitoa muun muassa osallistumalla erilaisten tilaisuuksien järjestämiseen.

Lisäksi virasto vastaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI)[90] ja sen asettamien riskienhallintaa, toiminnan jatkuvuutta, varautumista ja valmiutta, kyber- ja tietoturvaa sekä tietosuojaa kehittävien työryhmien toiminnasta.

---

[86] Tietosuojavaltuutetun toimisto: Apulaistietosuojavaltuutettu on tehnyt Opetushallitukselle aloitteen opetuksessa käytettävien sovellusten henkilötietojen käsittelystä. 26.2.2025 https://tietosuoja.fi/-/apulaistietosuojavaltuutettu-on-tehnyt-opetushallitukselle-aloitteen-opetuksessa-kaytettavien-sovellusten-henkilotietojen-kasittelysta

[87] Suomen kyberturvallisuusstrategia 2024–2035. 26.2.2025 https://julkaisut.valtioneuvosto.fi/handle/10024/165860

[88] Suomen kyberturvallisuusstrategian toimeenpanosuunnitelma. 28.2.2025 https://api.hankeikkuna.fi/asiakirjat/b9b35c4c-2719-4cfb-89fa-4388c855e2f0/c4785613-4037-43b5-b1cc-22d9b82c0d69/KIRJE_20241204070347.PDF

[89] Asiantuntijapalvelut tiedonhallintalautakunnalle. 2.3.2025 https://dvv.fi/asiantuntijapalvelut-tiedonhallintalautakunnalle

[90] Digi- ja väestötietovirasto, VAHTI. 26.2.2025 https://dvv.fi/vahti

VAHTI-johto- ja työryhmien tavoitteena on tukea ja koordinoida julkisen hallinnon digitaalisen turvallisuuden kehittämistä sekä yhteistyötä. Ne pyrkivät vahvistamaan digitaalisen turvallisuuden havainnointikykyä ja kyvykkyyksiä, vastaamaan erilaisiin uhkiin ja jakamaan ajantasaista tilannekuvaa yhteistyössä muiden viranomaisten kanssa. Lisäksi ne edistävät uuden teknologian turvallista käyttöönottoa julkisessa hallinnossa sekä tukevat kustannustehokasta kehittämistä kyber- ja digitaalisen turvallisuuden alueella.

VAHTI-johto- ja työryhmien keskeisiä tehtäviä ovat:

- Rakentaa ja vahvistaa yhteistyöverkostoja julkisen hallinnon palvelutuotannon ja turvallisuuden kehittämiseksi digitaalisen turvallisuuden eri osa-alueilla.
- Seurata kyberuhkien ja digitaalisen turvallisuuden kehitystä sekä edistää ajankohtaisen uhkatiedon jakamista julkisen hallinnon toimijoille yhteistyössä muiden viranomaisten kanssa.
- Julkaista hyviä käytäntöjä, tukimateriaaleja sekä muita materiaaleja ja järjestää seminaareja ja tilaisuuksia julkisen hallinnon digitaalisen turvallisuuden edistämiseksi.
- Tukea julkisen hallinnon organisaatioiden digitaalisen turvallisuuden osaamisen, tietoisuuden, asenteen ja kulttuurin kehittymistä.
- Tuottaa ajantasaista kokonaiskuvaa ja selvityksiä julkisen hallinnon kyber- ja digitaalisen turvallisuuden tilasta ja sen kehitystarpeista.

Digi- ja väestötietovirasto toteutti vuosina 2019–2023 valtiovarainministeriön rahoittaman JUDO-hankkeen, jossa kehitettiin erilaisia digiturvapalveluita. Julkisen hallinnon digiturvan kokonaiskuvapalvelun[91] avulla organisaatiot voivat vertailla oman hallinnollisen digiturvansa tasoa muihin toimijoihin. Lisäksi Digiturvallinen elämä -koulutukset sekä saman niminen peli[92] tarjoavat maksuttomia koulutuksia henkilöstölle ja asiantuntijoille. Sovellus on saatavilla iOS- ja Android-laitteille.

Taisto-digiturvaharjoituksia on järjestetty 2018 lähtien vuosittain.[93] Seitsemän vuoden aikana näihin joko puoli- tai kokopäivän työpöytäharjoituksiin on osallistunut yli 2200 harjoitustiimiä, joista valtaosa on ollut julkisen hallinnon organisaatioista sekä yli 14 000 johdon edustajaa tai asiantuntijaa.

Vuoden 2024 aikana Digi- ja väestötietovirasto käynnisti Digiturvan tietopankki-verkkopalvelun[94] osana uutta Suomi.fi-kehittäjille-alustaa. Tietopankki kokoaa keskeistä digitaalista turvallisuutta koskevaa materiaalia, kuten lainsäädäntö- ja muut velvoitteet sekä saatavilla olevat julkiset tukimateriaalit. Osana tätä kokonaisuutta on julkaistu myös opas digiriskien hallintaan.[95]

Ohjeet tietomurron uhriksi joutuneelle sekä muita tukipalveluita

Vastaamon tietomurto osoitti, kuinka tärkeässä roolissa ovat erilaiset ohjeet sekä muut tukipalvelut tietomurron kohteeksi joutuneille henkilöille, heidän läheisilleen ja organisaatiolle. Tapahtumasta kuluneiden viiden vuoden aikana tilanne on merkittävästi parantunut ja ohjeistusta on yhtenäistetty. Yhä useampi organisaatio tarjoaa nykyään

[91] Digiturvan kokonaiskuvapalvelu. 26.2.2025 https://www.suomi.fi/palvelut/digiturvan-kokonaiskuvapalvelu-digi-ja-vaestotietovirasto/1b38df61-ca48-41b4-a238-da5ab1baaf27
[92] Digiturvallinen elämä -koulutuskokonaisuus. 26.2.2025 https://dvv.fi/digiturvallinen-elama
[93] Taisto-harjoitus on mahdollisuus testata ja kehittää organisaationne digiturvaa. 26.2.2025 https://www.dvv.fi/taisto
[94] Suomi.fi kehittäjille: Digiturvan tietopankki. 26.2.2025 https://kehittajille.suomi.fi/palvelut/digiturva
[95] Suomi.fi kehittäjille: Digiturvan tietopankki. 27.2.2025 https://kehittajille.suomi.fi/oppaat/riskienhallinta

maksuttomia tukipalveluita. Lisäksi kaupalliset toimijat tarjoavat nettiyhteyksiä ja älylaitteita käyttäville kansalaisille maksullisia tietoturvapalveluita.

Digi- ja väestötietovirasto on laatinut oppaita tietomurron uhreiksi joutuneille. Opas *"Henkilötietojani on viety tai vuotanut"*[96] Suomi.fi-sivustolla tarjoaa ohjeita ja neuvoja henkilöille, joiden henkilötiedot ovat joutuneet vääriin käsiin tietomurron, tietovuodon tai identiteettivarkauden seurauksena. Se auttaa tunnistamaan väärinkäytön merkit, estämään tietojen vahingollisen käytön, tekemään tarvittavat kiellot ja hoitamaan tilanteen jälkiseuraukset. Oppaan sivustolla kävi toukokuussa 2024 kaikkiaan 138 000 vierailijaa, kesäkuussa 25 000 ja loppuvuoden 2024 kuuden kuukauden aikana yhteensä 67 000 vierailijaa. Opasta on päivitetty vuoden 2024 tietoturvaloukkausten perusteella ja uusien suojautumiskeinojen osalta.

Suomi.fi-sivuston opas *"Organisaatioltani on viety tai vuotanut tietoja"*[97] antaa ohjeita organisaatioille tietomurron tai tietovuodon sattuessa. Se neuvoo, miten toimia akuutissa tilanteessa, neuvoo estämään lisävahingot ja kehottaa ilmoittamaan viranomaisille. Lisäksi opas käsittelee jälkitoimia, kuten tietoturvan parantamista ja prosessien päivittämistä. Sivustolla on käynyt noin 7500 vierailijaa vuoden 2024 aikana.

Suomi.fi-sivuston opas "*Häiriö- ja kriisitilanteisiin varautuminen*"[98] tarjoaa tietoa ja ohjeita, miten valmistautua erilaisiin häiriöihin ja kriiseihin, kuten sähkökatkoihin, myrskyihin ja suuronnettomuuksiin. Sivustolla on käynyt marras-joulukuun aikana 950 000 vierailijaa.

Kyberturvallisuuskeskus on koonnut sivustolleen ohjeita ja oppaita yksityishenkilöille sekä työpaikoille tietoturvaosaamiseen[99] sekä käytännön neuvoja identiteettivarkauden uhriksi joutuneille.[100] Sivustolla selitetään, mikä identiteettivarkaus on ja miten rikolliset voivat käyttää henkilötietoja väärin. Sivusto neuvoo, miten voi suojautua taloudellisilta vahingoilta, tehdä rikosilmoituksen, asettaa vapaaehtoisen luottokiellon ja suojata tilinumeron. Lisäksi se ohjeistaa, miten voi estää tietojen väärinkäytön ja mistä saa apua kriisitilanteessa.

Kuluttajaliitto on julkaissut Helsingin kaupunkiin kohdistuneen tietomurron jälkeen sivullaan artikkelin ”Ohjeita tietomurron kohteeksi joutuneille”.[101] Artikkeli käsittelee vuotaneita tietoja, kuten henkilö- ja osoitetietoja, käyttäjätunnuksia ja sähköpostiosoitteita, sekä antaa neuvoja, kuten seurata omaa sähköpostia ja pankkiliikennettä epätavallisten tapahtumien varalta. Lisäksi suositellaan vaihtamaan salasanat ja käyttämään vahvoja, yksilöllisiä salasanoja eri palveluissa. Artikkeli ohjeistaa myös, miten toimia, jos tietoja käytetään väärin.

Rikosuhripäivystys (RIKU) on julkaissut sivullaan neuvoja tietomurron tai tietovuodon uhriksi joutuneille.[102] Sivustolla korostetaan, että on tärkeää seurata viranomaisten ohjeita ja tehdä tarvittavat sulkutoimenpiteet, jotta henkilötietoja ei käytetä petoksiin. RIKU tarjoaa myös keskusteluapua. Palvelut ovat maksuttomia.

---

[96] Suomi.fi: Henkilötietojani on viety tai vuotanut. 26.2.2025 https://www.suomi.fi/oppaat/tietovuoto
[97] Suomi.fi: Organisaatioltani on viety tai vuotanut tietoja. 26.2.2025 https://www.suomi.fi/oppaat/tietomurto
[98] Suomi.fi: Häiriö- ja kriisitilanteisiin varautuminen. 26.2.2025 https://www.suomi.fi/oppaat/varautuminen
[99] Kyberturvallisuuskeskus: Ohjeet ja oppaat yksityishenkilöille. 26.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille
[100] Kyberturvallisuuskeskus: Neuvoja identiteettivarkauden tai tietovuodon uhrille. 26.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-identiteettivarkauden-tai-tietovuodon-uhrille
[101] Kuluttajaliitto: Ohjeita tietomurron kohteeksi joutuneille. 26.2.2025 https://www.kuluttajaliitto.fi/materiaalit/ohjeita-tietomurron-kohteeksi-joutuneille/
[102] Rikosuhripäivystys: Tietomurto – neuvoja tietomurron tai tietovuodon uhriksi joutuneille. 26.2.2026 https://www.riku.fi/toimi-nain-jos-tietojasi-on-vuodettu-verkkoon/

Mieli ry[103] tarjoaa useita palveluja kansalaisille erityisesti mielenterveyden tukemiseksi. Tietomurron uhriksi joutuessa on mahdollista käyttää muun muassa kriisipuhelimen palvelua tai kriisikeskusten tarjoamaa tukea.

Sekasin-chat[104] on valtakunnallinen keskustelualusta 12–29-vuotiaille, joissa voi käydä luottamuksellisia keskusteluja mieltä askarruttavista asioista. Sekasin Kollektiivi on MIELI Suomen Mielenterveys ry:n, Suomen Punaisen Ristin, Setlementtiliiton ja SOS-Lapsikylän koordinoima yhteenliittymä, joka toimii nuorten mielen hyvinvoinnin edistämiseksi ja kriiseissä auttamiseksi.

KyberVPK[105] on suomalainen hakkerikollektiivi, joka perustettiin auttamaan kriittisten toimintojen tuottajia taistelussa hyökkäyksiä vastaan ja palautumaan niistä. Apua pyytävän organisaation tarpeitten mukaan se voi auttaa ennaltaehkäisemään tietoturvaongelmia, testata ympäristön turvallisuutta, ratkoa yhdessä tietoturvapoikkeamia tai esimerkiksi auttaa järjestelmien turvallisessa käyttöönotossa. Tämä vapaaehtoistyö ja maksuton toiminta on kohdistettu mm. sosiaali- ja terveydenhuoltoon, kuntiin, oppilaitoksiin ja muihin kriittisiä palveluita ja toimintoja tuottaviin organisaatioihin tai yrityksiin.

2.10 Muut selvitykset

Elisa Santa Monican tietomurtotutkintaraportti: Helsingin kaupunki teki 2.5.2024 sopimuksen Elisa Santa Monican kanssa tietomurron tutkinta-avusta. Osana toimeksiantoa kartoitettiin hyökkääjän toimia sisäverkossa sekä avustettiin Helsingin kaupunkia hyökkäyksen torjunnassa. Toimeksiantoa laajennettiin 7.5.2024 kattamaan koko tietoturvapoikkeaman selvitys sekä jatkuva KASKOn tietoturvavalvonnan tuki. Yritys tuotti 7.10.2024 laajan tutkintaraportin liitteineen, jossa on hyödynnetty myös ulkopuolisten tietoturvayritysten verkkolaitteisiin kohdistamaa forensiikkaa sekä palomuurien ja palvelimien lokiraportteja.

YK:n lapsen oikeuksien komitean yleiskommentti[106] ei käsittele suoraan tietosuojaa eikä tietoturvaa, mutta sopimuksen yleinen henki ja tavoitteet korostavat lapsen oikeutta yksityisyyteen ja turvallisuuteen, mikä kattaa myös tietosuojan ja tietoturvan.

Tietosuojavaltuutetun toimisto[107] on koostanut tietoa lasten tietosuojaoikeuksista. Tietosuojavaltuutettu korostaan, että jokaisella lapsella ja nuorella on oikeus tietosuojaan. Henkilötietoja ovat esimerkiksi nimi, osoite, syntymäpäivä, puhelinnumero, valokuvat ja videot sekä tiedot lääkärikäynneistä. Lapsilla on myös oikeus tietää, missä ja miksi heidän tietojaan käsitellään, sekä oikeus poistaa tai muuttaa tietojaan. Tietosuojavaltuutetun toimisto varmistaa, että lapsen etu otetaan huomioon henkilötietojen käsittelyssä.

Kansallisessa lapsistrategiassa[108] on nostettu esiin lapsen suojelu ja oikeus yksityisyyteen digitaalisissa palveluissa. Tämä näkökulma on osa laajempaa tavoitetta luoda lapsi- ja perhemyönteinen yhteiskunta, jossa lasten oikeudet toteutuvat kaikilla elämänalueilla.

Lastensuojelun keskusliitto on julkaissut verkkojulkaisun ”Lapsi verkossa - näkökulmia lasten oikeuksiin ja tietosuojaan digitaalisessa ympäristössä”[109], jossa käsitellään lasten

[103] Mieli ry. 26.2.2025 https://www.mieli.fi/
[104] Sekasin-chat. 26.2.2025 https://sekasin.fi/
[105] KyberVPK. 26.2.2025 https://kybervpk.fi/
[106] United Nations (2001) Convention on the Rights of the Child. 26.2.2025 https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/CRC_General_Comment_1_en.pdf
[107] Tietosuojavaltuutetun toimisto. Lasten tietosuojaoikeudet. 28.1.2025 https://tietosuoja.fi/lasten-tietosuoja
[108] Lapsistrategia. 26.2.2025 https:// lapsistrategia.fi/
[109] Lastensuojelun keskusliitto (2019): Lapsi verkossa – Näkökulmia lasten oikeuksiin ja tietosuojaan digitaalisessa ympäristössä. 26.2.2025 https://www.lskl.fi/wp-content/uploads/Lapsi-verkossa.pdf

oikeuksia ja tietosuojaa internetissä. Keskeinen viesti on, että lasten erityistarpeet ja oikeudet on huomioitava henkilötietojen käsittelyssä. Lapsilla on samat tietosuojaoikeudet kuin aikuisilla, mutta he tarvitsevat erityistä suojaa, kuten alle 16-vuotiaat huoltajan suostumuksen. Mainittu ikäraja on EU-tietosuoja-asetuksen 8 artiklan mukainen ikäraja, josta jäsenvaltio voi lainsäädännössään poiketa, kuitenkin niin, että ikäraja on vähintään 13 vuotta. Suomi on hyödyntänyt harkintamarginaalin. Tietosuojalain (1050/2018) 5 §:n mukaan tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettava ikäraja on (vähintään) 13 vuotta. Lisäksi korostetaan, että lapsille on tarjottava selkeää ja ymmärrettävää tietoa heidän henkilötietojensa käsittelystä.

Helsingin kaupungin sisäinen valvonta toteutti tietomurrosta kansliapäällikön tehtävänannon perusteella selvityksen. Selvitys valmistui 15.8.2024 ja sitä täydennettiin lisäselvityksellä 25.11.2024. Yhteenvedossa todetaan muun muassa, että VPN-reititin jäi toimintojen muuttuessa KASKOn vastuulle ja sen ylläpito laiminlyötiin. Käytössä ei ollut systemaattista konfiguraatioiden hallintaa eikä VPN-laitteen korvaaminen vaihtoehtoisella palvelulla edennyt joutuisasti. Keskitettyihin konesaleihin siirtymistä ei ollut muodostettu projektiksi KASKOssa ja muutosta toteutettiin lähinnä asiantuntijatyönä muiden työtehtävien yhteydessä. Muutosta ei pidetty kiireellisenä eikä palomuurin hälytyksille ollut aktiivista seurantaa. Reagointi tietomurtoon tapahtui viiveellä. Hälytyksiä poikkeavista havainnoista tuli jo noin viisi päivää ennen kuin tietomurto havaittiin ja siihen reagoitiin.

Tietomurtojen muiden digimaailmaan liittyvien hyökkäysten määrä on Kyberturvallisuuskeskuksen vuosiraportin mukaan joko kasvanut lievästi (tietomurron yritykset, tietovuodot) tai laskenut hieman (tietomurrot)[110]. Finanssiala ry:n[111] tuottamien tilastotietojen mukaan pankkien tietoon tulleet huijaukset ovat jatkaneet kasvua koko 2020-luvun ajan.

Helsingin kaupunkiin kohdistunut tietomurto on Suomen oloissa tähän mennessä merkittävin, koska kohteena on ollut noin 300 000 henkilöä, sisältäen perushenkilötietojen lisäksi joiltakin myös henkilötunnuksen sekä muita arkaluonteisia tietoja.

Verkkorikollisuus on muuttunut viimeisen vuosikymmenen aikana entistä ammattimaisemmaksi, globaaliksi liiketoiminnaksi. Verkkorikolliset ovat perustaneet CaaS-tyyppisiä (Crime-as-a-Service) palveluita, joissa tarjotaan kaikki tarvittavat työkalut ja muut palvelut avaimet käteen -periaatteella ja 24/7-asiakastuella varustettuna. Hyökkääjä voi pyytää sopivaa rikollistoimijaa kartoittamaan potentiaalisia kohteita, sen jälkeen hakemaan tarvittavan haavoittuvuuden ja hakemaan tarvittavan jalansijan, minkä jälkeen hyökkääjä voi käynnistää haluamansa kaltaisen hyökkäyksen, esimerkiksi kiristyksen varastamillaan tiedoilla.

Microsoftin vuosittaisessa Digital Defense 2024 -raportissa[112] todetaan, että World Economic Forumin mukaan verkkorikollisuus aiheutti yli 1000 miljardin dollarin vahingot vuonna 2023. Kuluttajien menetykset olivat 8,8 miljardia dollaria, missä oli nousua 30 % vuodesta 2022.

Julkiseen hallintoon kohdistuneita tietomurtoja tai palvelunestohyökkäyksiä on vuosilta 2018–2024 on koostettu seuraavaan taulukkoon (taulukko2):

---

[110] Kyberturvallisuus Suomessa 17.3.2025 https://kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuus-Suomessa.pdf

[111] Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta. 28.2.2025 https://www.finanssiala.fi/uutiset/huijaukset-rajussa-kasvussa-vuonna-2024-pankit-saivat-pysaytettya-huijattuja-maksuja-yli-44-miljoonan-euron-arvosta/

[112] Microsoft Digital Defense Report 2024 28.2.2025 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Taulukko 2: Tietomurtoja julkiseen hallintoon ja muihin merkittäviin toimijoihin 2018–2024.

Organisaatio	Ajankohta	Tapaus
Lahden kaupunki	2/2018	Cryptominer-louhintaohjelma Provincian verkossa.
Lahden kaupunki	6/2019	Haittaohjelma levisi tuhanteen työasemaan, selvittely- ja puhdistuskustannukset miljoona euroa.
Kokemäen kaupunki	8/2019	Kiristysohjelma lukitsi tiedostot. Palautuminen kesti pari viikkoa.
Porin kaupunki	8/2019	Kiristysohjelma havaittiin ajoissa (opetusverkko).
Siuntion kunta	9/2019	Tietomurto ja sen seurauksena kalasteluviestejä kunnan nimissä.
Turun kaupunki	4/2021	Tietomurto opetustoimen verkkoon. Kiristysohjelma havaittiin ajoissa.
Savonia AMK	2/2022	Tietomurrossa vietiin opiskelijoiden henkilötietoja, joita julkaistiin pimeässä verkossa.
KEUDA	11/2022	Lockbit-kiristysryhmä pysäytti Keski-Uudenmaan koulutuskuntayhtymän IT-ympäristön miltei kuukauden ajaksi. Kustannukset 100 000 euroa. Rahavaatimusta ei koskaan esitetty eikä tietoja vuodettu.
Säkylän kaupunki	12/2022	Ulkoisen palvelutuottajan virhe jätti aukon verkkoon. Tapausta ei ole kuvattu tarkemmin julkisuudessa.
Helsingin seudun liikenne	12/2022	Merkittävä määrä palvelunestohyökkäyksiä, useiden taustalla No-Name-niminen pro-Venäjä aktivistiryhmä. Sama ryhmittymä väittänyt hyökänneensä myös muihin julkisen hallinnon organisaatioihin vuosien 2022–2024 aikana.
Rautavaaran kunta	10/2023	Kiristysohjelma hallintoverkossa, hyökkääjä ehti kryptata osan tiedostoista.
Tietoevry Oyj	1/2024	Akira iski Tietoevryn datakeskukseen Ruotsissa ja tuhosi myös varmuuskopiot. Tapaus aiheutti isoja vahinkoja verkkokaupoille ja monille ruotsalaisille kunnille.
Helsingin kaupunki	4/2024	Tietomurto Helsingin kaupungin KASKOn verkkoon, jolloin tuntemattomaksi jäänyt hyökkääjä sai kopioitua arviolta 750 000 asiakirjaa.
Liikenne- ja viestintävirasto Traficom	5/2024	Väärinkäytös, jonka avulla ulkopuolinen taho pääsi lataamaan 65 000 ajoneuvon omistajan tai haltijan tietoja. Samaa menetelmää käytettiin myös Verohallinnon ylläpitämään positiiviseen luottotietorekisteriin. Tässä tapauksessa luotonantajan käyttämään ohjelmistoon tehty tietomurto, jonka seurauksena positiiviselta luottotietorekisteriltä kysyttiin oikeudettomasti luottotietorekisteriotteita.
Nordea	9/2024	Useita erittäin vakavia palvelunestohyökkäyksiä (DDoS) Nordea-pankkia vastaan, jotka haittasivat merkittävästi verkkopankin toimintaa sekä pankin tarjoamaa tunnistuspalvelua.

Vincit Oyj	12/2024	IT-yhtiö Vincitin työntekijän kotikoneen kautta tehty tietomurto, joka avasi hyökkääjälle pääsyn kymmenen asiakasyrityksen tietojärjestelmään. Hyökkääjä vei Valiolta suuren määrän henkilötietoja.

Selvitys 15 suurimman kunnan tietoturvallisuuden ja tietosuojan tasosta toteutettiin Vastaamon tietomurron jälkeen valtionhallinnossa kansallisista tietoturvan ja tietosuojan kehittämistarpeista. Selvitys oli osa valtioneuvoston periaatepäätöstä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (jäljempänä Titukri)[113]. Titukrin voimassaolo päättyi valtioneuvoston päätöksellä 10.10.2024.

Yhtenä periaatepäätöksen toimenpiteenä (toimenpide 29) haluttiin luoda kattavampi tilanneymmärrys Suomen 15 väkiluvultaan suurimman kunnan sekä niiden alueella toimivien kriittisen infrastruktuurin toimijoiden tietoturvan ja tietosuojan tasosta. Kriittisen infrastruktuurin osalta kiinnostuksen kohteena olivat sosiaali- ja terveydenhuollon sekä energia- ja vesihuollon toimijat. Kerrotuin kriteerein tunnistettuja organisaatioita oli 66, joista selvitykseen osallistui 41.

Selvityksen toteutuksesta vastasivat valtiovarainministeriö ja Kyberturvallisuuskeskus. Valtiovarainministeriö vastasi selvitysprojektin kokonaisohjauksesta.

Kyberturvallisuuskeskus vastasi energiayhtiöiden ja vesilaitosten aineistojen keräämisestä ja kuntien hyökkäyspintakartoituksesta sekä osallistui selvitystyön ohjaukseen sekä raportin suunnitteluun, kommentointiin ja kirjoittamiseen. Digi- ja väestötietovirasto tuki valtiovarainministeriötä vastaamalla kuntien ja hyvinvointialueiden aineistojen keräämisestä sekä osallistui raportin suunnitteluun ja kirjoittamiseen. Kaksi konsulttiyhtiötä tuki selvityksen vastuutahoja – toinen aineistojen keräämisessä ja toinen raportin laatimisessa.

Selvitys on turvallisuusluokiteltu ja tarkoitettu toiminnan kehittämiseen vastuuviranomaisissa ja selvityksen kohteina olleissa organisaatioissa. Tutkintaselosteeseen nostetaan kuitenkin kehittämisehdotuksia, jotka yleisellä tasolla kuvailevat ilmiötä paljastamatta salassapidon piiriin kuuluvia asioita.

Selvityksen keskeisissä tuloksissa todetaan muun muassa, että kunnallisella tasolla:

- kuntia tulee tukea keskeisen suojattavan omaisuuden tunnistamisessa
- toimitusketjujen riskienhallinta on puutteellista, millä tarkoitetaan muun muassa yhtiöitettyjen tai ulkoistettujen palvelujen varautumista.

Valtakunnallisella tasolla:

- tulisi kiinnittää huomioita siihen, että olemassa olevia menetelmiä ja selvityksiä käytettäisiin laaja-alaisesti toiminnan kehittämisessä (kyberkypsyysselvitykset, digiturvakysely)
- käytössä olevia palveluja saataisiin laajennettua kuntien käyttöön aiempaa paremmin (erityisesti Hyöky-palvelu)
- ennalta ehkäisevien, toimintaa kehittävien ja mittaavia työkaluja ja menetelmiä tulisi käyttää ja kehittää laajemmassa viranomaisyhteistyössä
- palvelujen käyttöön velvoittamista kansallisella lainsäädännöllä tulisi arvioida.

Opetustoimi ei ollut selvityksen kohteena, koska sitä ei katsota em. periaatepäätöksen toimeenpanossa yhteiskunnan kriittiseksi toimialaksi. Periaatepäätöksen valmisteluvaiheessa

[113] LVM/2021/44.

Opetushallituksen antamassa lausunnossa (3.3.2021) todetaan, että Opetushallitus ehdottaa päätösluonnoksessa selvityksen kohteeksi esitettyjen toimialojen lisäksi myös Suomen 15 suurimman kunnan tietoturvan ja tietosuojan tason selvittämistä opetustoimessa. Edelleen lausunnossa todetaan, että opetustoimessa on paljon alaikäisten lasten tietoja sekä lisääntyvässä määrin erityisiä henkilötietoja (kuten tiedot erityisen tuen tarpeesta), joten tietoturvasta ja tietosuojasta huolehtiminen on tärkeää.

Kuntaliitto on kyberturvallisuuden edistämiseksi kunnallishallinnossa laatinut erilaisia selvityksiä ja oppaita. Raportti *"9 Digiturvaan liittyvää haastetta kuntajohdolta"*, joka on julkaistu vuonna 2021, kokoaa kuntajohdon käsityksiä digiturvallisuuden tilanteesta kunnista. Raportin mukaan muun muassa:

- kunnista puuttuu digiturvan toimintamalli, joka ohjaisi digiturvallisuuden johtamista ja toteuttamista kunnissa
- kyky reagoida äkillisissä hyökkäystilanteissa on puutteellinen
- osaaminen keskittyy liiaksi, aihealueen sisältö on usein teknologista ja vaikeasti ymmärrettävää
- digiturvallisuuden vaatimukset heikentävät usein sujuvuutta ja käytettävyyttä.

Selvityksen mukaan kunnissa tarvitaan laaja-alaisempaa osaamista digiturvasta, eikä kaikkea osaamista ole mahdollista keskittää yksittäisiin kuntiin. Siksi Kuntaliiton ja muiden yhteistyötahojen tuki on kunnille tärkeää.

Kuntaliitto on laatinut myös *"Digitaalisen turvallisuuden muistilistan kuntajohtajille*". Muistilistassa on lyhyesti lueteltu keskeiset vastuutettavat asiat sekä esitetty tukea antavat viranomaiset ongelmatilanteissa.[114] Muistilistalla ei kuitenkaan tuoda esille esimerkiksi sitä, että usein tietoverkkoihin kohdistuneen hyökkäyksen torjunta ja selvittäminen vaatii erityisosaamista, jota on saatavilla lähinnä tietoturvapalveluja tuottavilta yrityksiltä.

Kuntaliitto julkaisi vuonna 2023 kunnille *hallintosääntömallin.*[115] Hallintosääntö on kuntalain edellyttämä kunnan johtamista ja hallintoa määrittelevä kunnan sisäinen säännöstö. Hallintosääntömallin 9. luvussa esitetään tiedonhallintaa ja tietoturvaa koskevien vastuiden järjestämisen perusteet kunnassa.

Selvitys tietoverkkorikollisuuden torjunnasta on sisäministeriön julkaisu vuodelta 2017. Selvityksessä esitetään toimenpide-ehdotuksia, jotka koskevat muun muassa verkkorikosten torjunnan kehittämistä, torjuntaan liittyvän koulutuksen parantamista, verkkorikollisuuden tilannekuvatoiminnan kehittämistä sekä lainsäädännön uudistamista. Selvityksen toimenpide-ehdotusten toteutuminen ei ollut enää aktiivisessa seurannassa, joten tutkintaryhmä pyysi ministeriön poliisiosastoa laatimaan yhteenvedon toimenpiteiden etenemisestä.

Poliisiosaston laatimasta yhteenvedosta käy ilmi, että keskeiset toimenpide-ehdotukset ovat edenneet. Uudistuksia on tehty varsinkin yhteistyörakenteissa ja koulutuksessa. Muun muassa Poliisiammattikorkeakoulun opetustarjontaan on kehitetty aihealueen tutkintaan liittyvää koulutusta.

Lainsäädännössä on niin ikään tapahtunut tai tapahtumassa kehitystä. Lainsäädäntöä koskeneissa toimenpide-ehdotuksissa oli nostettu esille verkkorikollisuuden esitutkinnan toimittamisvelvollisuuteen kohdistamat paineet. Toimenpide-ehdotus kuului seuraavasti:

---

[114] Kuntaliitto: Digitaalisen turvallisuuden huoneentaulu kuntajohtajalle. 26.2.2025 https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntajohtajan_muistilista_digiturvallisuus_0.pdf

[115] Kuntaliitto: Hallintosääntömalli. 26.2.2025 https://www.kuntaliitto.fi/julkaisut/2023/2239-kunnan-hallintosaantomalli

”Arvioidaan yhdessä oikeusministeriön kanssa poliisin esitutkinnan toimittamista koskevien säännösten muutostarpeita sekä tarvittaessa valmistellaan lainsäädäntömuutoksia niin, että tutkintavoimavarat voidaan kohdistaa asianmukaisesti ottaen huomioon tietoverkkoympäristöön kohdistuvien rikosten laatu ja asianomistajan asema.”

Poliisiosaston yhteenvedossa tuodaan esille, että Vastaamon ja WinCapitan tapaukset osoittavat, ettei Suomessa ole mekanismia, jolla voitaisiin kollektiivisesti huolehtia rikoksen uhrien oikeuksista. Se haastaa viranomaisten kykyä käsitellä tapauksia, jossa on suuri määrä asianomistajia. Suomalainen rikosprosessi ja sen prosessisäännöt eivät taivu suurten asianomistajamäärien ja heidän yksityisoikeudellisten vaatimustensa käsittelyyn.

Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa on sisäministeriön ja puolustusministeriön 15.2.2022 asettama sisäisen turvallisuuden ja puolustusselontekojen linjausten sekä aiemmin valtioneuvoston periaatepäätöksen 10.6.2021 mukainen yhteinen selvityshanke viranomaisten toimintaedellytysten arvioimiseksi kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuvan kehittymisen.[116] Selvityksen tavoitteena oli laatia kehittämisehdotuksia, joiden avulla voidaan parantaa viranomaisten toimintaedellytyksiä.

Selvityksen mukaan reaalimaailmassa viranomaisilla on yleensä selkeät tehtävät eri uhkatilanteiden hallinnassa ja viranomaisten väliset vastuualueet sekä yhteistyövelvoitteet on määritelty. Kybertoimintaympäristön osalta Suomessa ei ole laissa riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta eri tasoilla, eikä lainsäädäntö ota tarvittavassa määrin huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa.

Kybertoimintaympäristön suojaaminen on jakaantunut usealle eri hallinnonalalle eikä koko kybertoimintaympäristöä ole osoitettu eikä voida osoittaa yhdenkään hallinnonalan tehtäväksi. Uhkiin reagoiminen edellyttää tiivistä hallinnonalojen välistä yhteistyötä niin strategisella kuin operatiivisellakin tasolla. Yhteistyötä entisestään tiivistämällä voitaisiin varmistaa, että oikea viranomainen suorittaa toimenpiteitä oikeaan aikaan kuitenkaan vaarantamatta toisen viranomaisen tehtäviä ja että toiminnassa saadaan käyttöön paras osaaminen.

Selvityksen mukaan nykytilassa viranomaisilla ei ole riittäviä toimintaedellytyksiä tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Toimintaedellytysten parantamiseksi on tunnistettu kehittämistoimenpidetarpeita seitsemältä keskeiseltä osa-alueelta: kyberturvallisuuden strateginen tavoitetila, yhteistoiminta ja viranomaisprosessit, tilannekuva, tiedonvaihto, vaikuttaminen ja vastatoimet, tiedonhankinta ja viranomaisverkkojen suojaus.

Viranomaisyhteistyön tiivistämistarpeen ohella on syytä ottaa huomioon se, että monet yhteiskunnan kriittisistä toiminnoista ovat vahvasti yksityisen sektorin omistuksessa ja vaihtelu näiden toimijoiden kyberturvallisuusvalmiuksissa on merkittävää. Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team) avustaa tarvittaessa ensivaiheessa toimijoita tietoturvaloukkausten selvittämisessä, mutta laajempi selvittäminen ja jatkotoimet toteutetaan esimerkiksi yksityisen sektorin palveluja hyödyntäen.

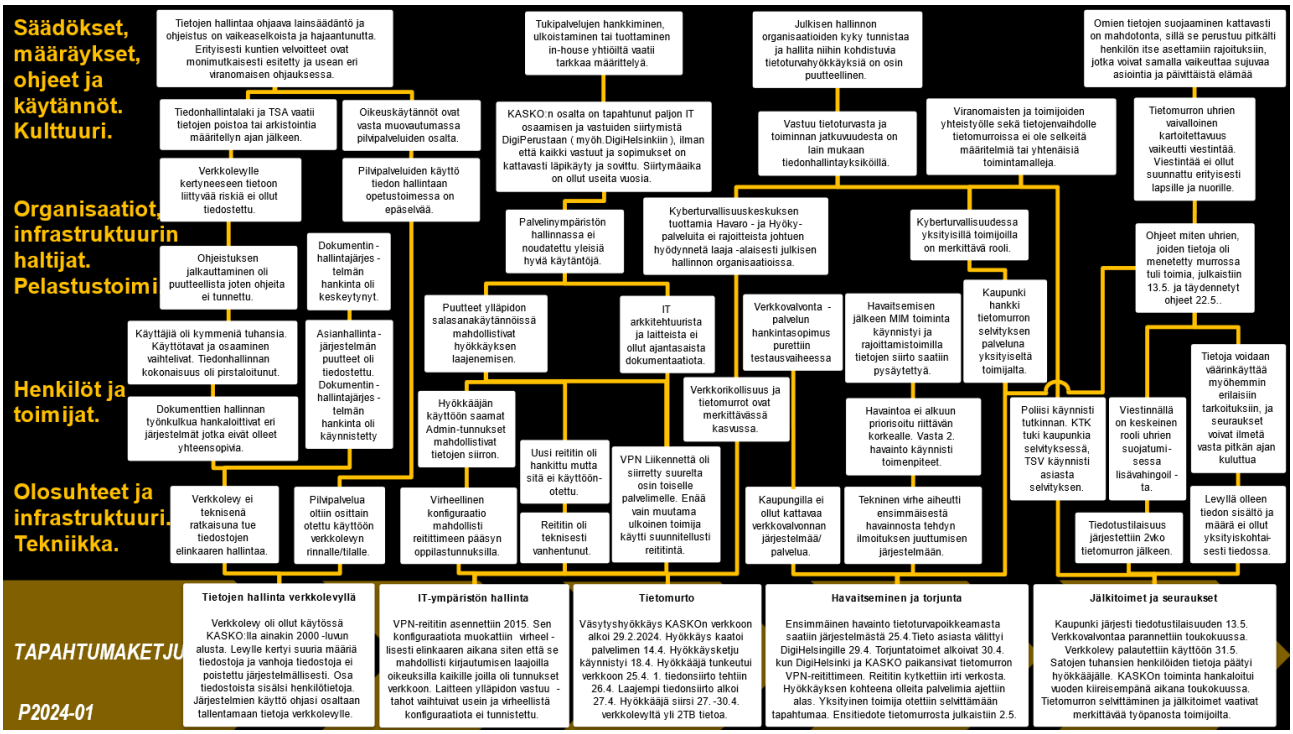
---

[116] Valtioneuvosto (2023): Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164793/VN_2023_31.pdf

3 ANALYYSI

Tapahtuman analysoinnissa on käytetty Onnettomuustutkintakeskuksen edelleen kehittämää Accimap-menetelmää.[117] Analyysitekstin jäsentely perustuu tutkinnassa laadittuun Accimap-kaavioon, jossa tapahtuma kuvataan kaavion alaosassa tapahtumaketjuna. Tapahtumaketjun taustalta paljastuvia tekijöitä puretaan kaaviossa eri analyysitasoilla.

3.1 Tapahtuman analysointi



Kuva 18. P2024-01 ACCIMAP-analyysikaavio.

3.2 Tietojen hallinta verkkolevyllä

Helsingin kaupungin kasvatuksen ja koulutuksen toimialalla (KASKO) otettiin 2000-luvun alussa käyttöön verkkolevy, jolle voitiin tallentaa tiedostoja hyvin vapaasti. Levylle oli pääsy kaikilla KASKOn työntekijöillä ja, sillä oli vuosien varrella kymmeniä tuhansia käyttäjiä. Levylle kertyi vuosien aikana yli neljä miljoonaa tiedostoa, joista osa sisälsi arkaluonteisia, erityisiin henkilötietoryhmiin kuuluvia tietoja. Levyn sisältöä ei vuosien aikana käyty järjestelmällisesti läpi eikä vanhoja tiedostoja poistettu. Verkkolevyt teknologiana ovat olleet pitkään yleisesti käytössä, mutta ne eivät teknisenä ratkaisuna tue järjestelmällistä tiedonhallintaa eivätkä tiedon elinkaarimallia.

Verkkolevylle jouduttiin tallentamaan toimintaa tukevaa ja päätöksenteon valmisteluun liittyvää aineistoa, jota hyödynnettiin myös käytössä olleissa virallisissa asianhallintajärjestelmissä. Tämä johtui Helsingin kaupungin monista tietojärjestelmistä, joita ei ollut integroitu yhtenäiseksi asianhallintakokonaisuudeksi.

---

117 Rasmussen, J. & Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.

Helsingin kaupungilla oli henkilöstölle ohjeistusta tiedonhallintaan ja IT-ympäristön käyttöön. Ohjeet olivat osin hajallaan kaupungin dokumenttienhallintajärjestelmissä. Keskeinen ongelma oli ohjeiden heikko tunnettuus KASKOn henkilöstön keskuudessa, joten niiden vaikutus käytännön toimintaan oli vähäinen.

Helsingin kaupunki oli tunnistanut puutteita asiakirjahallintajärjestelmissään ja käynnistänyt tähän liittyvän julkisen hankinnan. Markkinaoikeus kuitenkin kumosi hankinnan muotovirheen vuoksi.

Helsingin kaupungilla oli osittain siirrytty käyttämään pilvipalveluita verkkolevyjen sijaan. KASKO oli kuitenkin jatkanut verkkolevyjen käyttöä suuressa osassa organisaatiotaan. Pilvipalveluiden käyttöönottoa kuntasektorilla ovat osaltaan hidastaneet epäselvyydet niiden käytön oikeudellisista edellytyksistä ja rajoituksista. Myös oikeuskäytännöt ovat vasta muotoutumassa.

Verkkolevyn käyttöoikeudet oli määritelty organisaatio- ja toimintokohtaisesti, samoin tiedostojen varmuuskopiointi oli järjestetty, mutta levylle kertyneeseen suureen tiedostomäärään tai sen vuotamiseen liittyviä riskejä ei tiedostettu.

Tiedonhallintaan liittyy paljon lainsäädäntöä, ohjeistusta ja useita viranomaisia. Aihe on hajaantunut useisiin lakeihin ja kokonaisuutta on vaikea hahmottaa. Tiedonhallintalaki ja EU:n yleinen tietosuoja-asetus määräävät poistamaan tai arkistoimaan tallennetun tiedon organisaation niille määrittelemässä ajassa.

3.3 IT-ympäristön hallinta

Tietomurto kohdistui VPN-reitittimeen, joka oli otettu käyttöön vuonna 2014. Etäyhteydet KASKOn verkkoon oli pääosin siirretty jo muille VPN-reitittimille, joten murron kohteeksi joutunutta ASA 5515 -reititintä käyttivät lähinnä ulkoiset toimijat. Laite oli teknisesti vanhentunut ja puuttuvien päivitysten vuoksi sen tietoturva ei ollut ajan tasalla. Reitittimelle oli hankittu korvaava laite, mutta sitä ei ollut otettu käyttöön.

Ratkaisevin tekijä tietomurron onnistumiselle oli virheellinen konfiguraatio, joka mahdollisti pääsyn järjestelmään oppilastunnuksilla ja antoi laajat-oikeudet sisäverkon käyttöön. Asetusmuutoksen ajankohtaa tai tekijää ei tutkinnassa pystytty selvittämään. Laitteen ylläpidon vastuut olivat vaihtuneet useita kertoja ja olivat tietomurron hetkelläkin epäselvät.

Hyökkääjän sisäverkosta haltuunsa saamat ylläpitotunnukset sekä puutteet salasanakäytännöissä helpottivat tietomurron laajentamista uusille palvelimille. Kokonaisuutena tietoliikenne- ja palvelinympäristön hallinnassa ei noudatettu IT-alan hyviä käytäntöjä.

Helsingin kaupungin IT-palveluiden organisointia oli järjestetty uudelleen viimeisen viiden vuoden aikana. Niitä oli keskitetty ensin Digitaaliseen perustaan ja myöhemmin DigiHelsinki-yhtiöön. KASKO toimialana oli jatkanut pääosin oman tietoteknisen kokonaisuuden ylläpitämistä. Sen sisällä oli kuitenkin tapahtunut paljon organisaatio- ja henkilömuutoksia, joiden seurauksena KASKOn tietotekniikan ylläpitovastuut olivat osin epäselviä. Kuntasektorilla on yleisesti tunnistettu ulkoisten palveluiden hankkimisen, ulkoistamisen ja in-house yhtiöiden käyttämisen haasteet palveluiden tuottamisessa.

3.4 Tietomurto

Tietomurtoa oli valmisteltu helmikuun 2024 lopussa ja maaliskuussa tehdyllä väsytyshyökkäyksellä sekä ympäristön skannauksella. KASKOn käyttämään VPN-reitittimeen kohdistettiin 14.4.2024 hyökkäys tunnettua haavoittuvuutta käyttäen, mikä kaatoi

reitittimen. Kaatumisen syytä ei kuitenkaan tutkittu, vaikka tutkinta olisi paljastanut laitteen olevan yhä käytössä ja päivittämätön sekä sen, että laitteen lokitus ei toiminut erillisen lokipalvelimen levytilan täyttymisen takia.

Varsinainen tietomurto käynnistyi 18.4.2024. Hyökkääjä kirjautui KASKOn verkkoon reitittimen kautta 25.4.2024, jolloin tehtiin ensimmäinen tiedostosiirto ulos verkosta. Merkittävimmät tiedostosiirrot tehtiin 27.-30.4.2024 välisenä aikana, jolloin tietoa vietiin yhteensä noin kaksi teratavua (noin 750 000 tiedostoa).

Tietomurrot ovat yleisesti olleet kasvussa viime vuosina. Kyberturvallisuuskeskus tuottaa tilannekuvaa yhteiskunnalle ja organisaatioille Havaro- ja Hyöky-palveluiden avulla. Helsingin kaupunki on ollut Hyökyn asiakas vuoden 2023 lopusta alkaen, mutta haavoittuva reititin oli jätetty pois palvelun tekemistä tarkistuksista.

Kyberturvallisuuskeskuksen tuottamia palveluita ei hyödynnetä laajasti julkisen sektorin organisaatioissa, koska Kyberturvallisuuskeskuksella ei ole ollut resursseja kehittää ja ylläpitää näitä palveluita tälle kohderyhmälle.

Verkkorikollisuus aiheuttaa merkittävää uhkaa julkiselle hallinnolle, jolla on hallussaan suuria määriä kansalaisista kerättyjä tietoja. Siksi julkiset organisaatiot voivat olla houkuttelevia tietomurron kohteita. Useimmiten tietojen käsittely julkisessa hallinnossa perustuu lakisääteisen tehtävän hoitamisen, minkä vuoksi rekisteröityjen ihmisten mahdollisuudet rajoittaa ja valvoa omien tietojensa käyttöä ovat rajalliset. Hallinnon asiakkaan alisteisen aseman takia julkiselle hallinnolle muodostuu korostunut velvollisuus suojata rekisteröityjen tietoja.

Organisaation johdon vastuu tietoturvallisuudesta ja tietosuojasta on yksiselitteinen.

3.5 Havaitseminen ja torjunta

Haittaohjelmien tunnistusohjelma antoi hälytyksiä 25.4.2024, mutta tieto niistä välittyi KASKOlle vasta 29.4.2024. Tietoturvahälytysten kriittisyyttä ei silloinkaan heti tunnistettu, joten torjuntatoimet pääsivät alkamaan vasta 30.4.2024.

KASKO ja DigiHelsinki paikansivat tietomurron lähteenä olevan VPN-reitittimen, joka irrotettiin verkosta, ja hyökkäyksen kohteena olleet muut palvelimet ajettiin alas. Viiveeseen ensimmäisestä havainnosta torjuntatoimien käynnistämiseen vaikuttivat tekniset ja prosessivirheet palvelupyyntöjärjestelmässä sekä tiedonkulun puutteet toimijoiden välillä.

Mikäli käytössä olisi ollut kattava lokienhallinta ja tietoturvavalvomo, hyökkäys olisi todennäköisesti tunnistettu jo valmisteluvaiheessa, eikä se olisi edennyt tietomurtoon asti. Reaaliaikainen verkkovalvonta olisi havainnut yöaikaan tapahtuvat poikkeuksellisen suuret tiedonsiirrot sisäverkosta internet-verkkoon. Helsingin kaupunki oli hankkimassa kattavaa verkkovalvonnan järjestelmää, mutta sen hankinta oli keskeytynyt, koska tilaaja ei ollut tyytyväinen käyttöönottotestauksen tuloksiin.

Koska kaupungin omat resurssit ja osaaminen havaittiin riittämättömiksi, tietomurron selvittämiseksi ja hallitsemiseksi ostettiin palvelua ulkopuoliselta yritykseltä. Tietoturvallisuudessa kriittiset resurssit ovat yksityisillä toimijoilla ja viranomaisten käytössä olevat resurssit ovat rajalliset. Julkisen sektorin toimijoilla ei ole mahdollista tukea laajasti toimijoita tietomurroissa tai muissa tietoturvallisuuteen liittyvissä kriisitilanteissa. Viranomaisten keskinäinen yhteistoiminta on näissä tilanteissa osin jäsentymätöntä eikä aina tue häiriötilanteen hallintaa.

Helsingin kaupunki perusti useita työryhmiä, jotka kokoontuivat säännöllisesti ja tiheästi kriisitilanteen hallitsemiseksi. Kaupunki käynnisti julkisen tiedottamisen mediatiedotteella 2.5.2024. Alkuperäinen tilannekuva tapahtuneesta, sen seurauksista ja vaikutuksista eri kohderyhmille tarkentui tietomurron selvitystyön edetessä.

Tietomurroissa huomio keskittyy helposti tapahtuman teknisiin yksityiskohtiin, kuten järjestelmien haavoittuvuuksiin ja tietoturvatoimenpiteisiin. Viestinnän rooli on kuitenkin yhtä kriittinen – se vaikuttaa suoraan uhrien mahdollisuuteen suojautua lisävahingoilta. Selkeä, nopea ja johdonmukainen viestintä auttaa hallitsemaan tilannetta, ehkäisemään väärää tietoa ja varmistamaan, että asianomaiset saavat tarvitsemansa tuen ja ohjeet.

3.6 Jälkitoimet ja seuraukset

Tiedotustilaisuus järjestettiin 11 päivää myöhemmin 13.5.2024. Siinä annettiin ohjeita ja kerrottiin, että tilannetta ja sen laajuutta selvitetään edelleen. Tiedotteessa 21.5.2024 kerrottiin, että tietomurron uhrina olleet kohderyhmät ovat laajentuneet.

Viestinnässä ei voi jäädä odottamaan selvitystyön lopullisia tuloksia, vaan on tärkeää antaa varhaisessa vaiheessa yleiskuva ja kertoa suojaustoimista tietomurron uhreille. Vaikka tietomurroissa joudutaan toimimaan vajavaisin tiedoin, avoimuudella rakennetaan luottamusta ja vältetään informaatiotyhjiön syntyminen ja spekulaatioiden leviäminen.

Helsingin kaupunki kohdensi nopeasti viestintää kaupungin työntekijöille ja huoltajille. Henkilökohtaista ja vuorovaikutteista viestintää tukemaan avattiin palvelunumero tietomurron uhreille ja asianosaisille, kuten huoltajille. Viestintää ei kuitenkaan kohdennettu eri ikäryhmille, kuten lapsille ja nuorille heidän ikätasonsa mukaisesti, eikä siinä huomioitu lasten ja nuorten tarpeita esimerkiksi selkeän kielen (myös vähemmistökieliryhmät), visuaalisen sisällön tai heidän käyttämien viestintäkanavien kautta. Esimerkiksi kattava ja tehokas tapa tavoittaa alaikäiset on koululuokittain, sillä se mahdollistaa tiedottamisen suoraan oppilaille ikätasolle sopivalla tavalla sekä tarjoaa samalla tilaisuuden kysymyksiin ja ohjaukseen.

Helsingin kaupunki tiedotti 18.6.2024, että kaupunkiin kohdistunut tietomurto ei ole laajentunut. Kaupunki tiedotti 12.7.2024, että valtioneuvoston nimittämä tutkintaryhmä aloittaa tutkinnan Helsingin kaupunkiin kohdistuneesta tietomurrosta. Seuraavan kerran kaupunki tiedotti tietomurron tilanteesta 17.12.2024.

Tietosuoja-asetuksen (GDPR) 34 artiklan mukaisesti tietoturvaloukkauksen uhrien tiedottaminen on ensisijaisesti toteutettava henkilökohtaisesti ja ilman aiheetonta viivytystä, mikäli loukkaus todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille tai vapauksille.

Helsingin kaupunki kohdensi nopeasti sisäistä viestintää kaupungin työntekijöille. Kaupungin työntekijöiden tavoittaminen onnistui nopeasti henkilökohtaisen viestinnän kautta, koska heidän sähköpostiosoitteensa olivat tiedossa ja heille voitiin ilmoittaa viivytyksettä tietomurrosta sekä kaupungin intranetissä että henkilökohtaisella sähköpostiviestillä. Henkilökohtaista ja vuorovaikutteista viestintää tukemaan avattiin palvelunumero tietomurron uhreille ja asianosaisille.

Entisten ja nykyisten oppijoiden, heidän huoltajiensa sekä muiden kaupungin kanssa asioineiden tavoittaminen osoittautui huomattavasti vaivalloisemmaksi. Henkilökohtainen tiedottaminen kaikille rekisteröidyille koettiin olevan mahdotonta, eikä sitä yritetty. Vaikka tietosuoja-asetus sallii yleisen tiedoksiannon käytön silloin, kun yksilökohtainen tavoittaminen olisi kohtuutonta, tämä ei automaattisesti takaa tiedotuksen vaikuttavuutta tai kattavuutta.

Tietomurron uhriksi joutuminen voi aiheuttaa monenlaisia terveydellisiä riskejä, henkistä kuormitusta ja turvallisuuden tunteen järkkymistä. Varastettuja tietoja voidaan hyödyntää rikollisiin tarkoituksiin, kuten identiteettivarkauksiin, taloudellisiin petoksiin, kiristykseen ja huijauksiin sekä maineen vahingoittamiseen vuosienkin jälkeen. Väärinkäytön vaikutukset eivät välttämättä ilmene heti.

Alaikäiset eivät välttämättä pysty eivätkä osaa suojata omia tietojaan. He voivat olla myös tietämättömiä tietosuojan tärkeydestä. Heillä ei välttämättä ole tietoa siitä, miten tietoja voidaan käyttää rikollisiin tarkoituksiin, eivätkä he aina ymmärrä suojautumisen tärkeyttä. Lisäksi suojaustoimenpiteet, kuten luottokiellot tai tietojen poistopyynnöt, voivat olla monimutkaisia alaikäisen näkökulmasta ja ne vaativat huoltajan toimenpiteitä. Vastaavasti ne voivat olla haasteellisia myös niille henkilöille, jotka eivät puhu suomea, ruotsia tai englantia.

On tärkeää, että nuorille ja heidän huoltajilleen tarjotaan selkeää ja saavutettavaa ohjeistusta tietomurtoihin varautumisesta ja niiden seurausten minimoimisesta. Lisäksi koulutuksen ja mediakasvatuksen kautta voidaan auttaa nuoria ymmärtämään, miten heidän tietojaan voidaan käyttää ja miten he voivat suojata itseään paremmin.

Tämän selostuksen valmistumiseen mennessä ei ole havaittu merkkejä siitä, että henkilötietoja olisi levitetty pimeässä verkossa tai hyödynnetty identiteettivarkauksissa. Tietojen hyödyntämistä tulevaisuudessa ei kuitenkaan voida sulkea pois.

4 JOHTOPÄÄTÖKSET

Johtopäätökset sisältävät tapahtuman syyt. Syyllä tarkoitetaan erilaisia tapahtuman taustalla olevia tekijöitä ja siihen vaikuttavia välittömiä ja välillisiä seikkoja.

1. Verkkolevylle kertyi vuosien saatossa erilaisia tietoja ja tarpeettomaksi käyneiden tietojen poistaminen perustui ihmisten oma-aloitteeseen tietojen poistamiseen ja tiedostojen järjestelyyn, eikä se ollut järjestelmällistä eikä valvottua.

   Johtopäätös: *Tiedon elinkaaren hallinnan perustuminen käyttäjien itsensä toteuttamiin hallintatoimiin altistaa tilanteelle, jossa tietojenkäsittelyn ja tiedon hallinnan kokonaisuudesta muodostuu hallitsematon.*

2. Tiedonhallintalaki ja tietosuoja-asetus ovat keskenään yhteensovitettuja, mutta yhdessä muiden julkisen hallinnon säädösten, kuten hallintolain, julkisuuslain, arkistolain ja erityislainsäädännön kanssa tiedonhallinnan kokonaisuus näyttäytyy vaikeaselkoisena, ja eri lait sisältävät useita samankaltaisia arviointi- ja suunnitteluvelvollisuuksia.

   Johtopäätös: *Julkisen hallinnon tiedonhallintaan liittyy useita eri ajankohtina annettuja säädöksiä, jotka eivät muodosta selkeästi yhteensovitettua kokonaisuutta. Tämän vuoksi tiedonhallinnasta vastaavien on hankala hahmottaa vaatimusten kokonaisuutta ja se johtaa näiden vaihtelevaan soveltamiseen.*

3. Julkisen hallinnon tiedonhallintaa, tietoturvaa ja tietosuojaa ohjaavat useat eri viranomaiset. Viranomaiset suorittavat ohjausta itsenäisesti, oman tehtävänsä mukaisista lähtökohdista.

   Johtopäätös: *Useiden viranomaisten ohjatessa tiedonhallintaa, tiedonhallintayksiköiden saama ohjaus on hajautunutta ja käytännössä säädösten ja ohjeiden soveltaminen vaihtelee. Viranomaisten suorittama työ on ohjausta, mutta toimijoiden valvonta on vähäistä.*

4. Tietoverkkorikollisuus on kasvava rikollisuuden ala ja sen aiheuttamat haitat ovat merkittäviä. Julkinen hallinto on sillä olevien tietojen laadun ja määrän takia rikollisia kiinnostava kohde.

   Johtopäätös: *Julkisen sektorin kyky vastata tietoverkkorikosten aiheuttamiin uhkiin on tällä hetkellä puutteellinen, koska hyökkäysten ja haavoittuvuuksien havainnointimenetelmiä ei ole käytössä kattavasti. Hyökkäysten ja haavoittuvuuksien tunnistamisella ja korjaamisella on mahdollista estää tietomurtoja ja suojata tietoja.*

5. Vanhentunut VPN-reititin jäi käyttöön, vaikka valtaosa sen käyttäjistä oli siirtynyt uuteen VPN-reitittimeen. Laite ei kuulunut selkeästi kenenkään vastuulle, joten sen ylläpito oli minimaalista ja rajoittui vain pakolliseen varmenteen uusimiseen.

   Johtopäätös: *Tekniikan ja organisaation muuttuessa IT-laitteita jää heikolle ylläpidolle, jolloin ne muodostavat riskin tietomurroille.*

6. Tietomurron valmistelu olisi ollut mahdollista havaita useita viikkoja aikaisemmin kattavalla verkkovalvonnalla. Yritykset laajentaa murtoa sisäverkossa aiheuttivat hälytyksiä, mutta niihin ei reagoitu riittävästi.

   Johtopäätös: *Tietomurron onnistuminen johtuu harvoin yhdestä virheestä tai laiminlyönnistä. Verkkovalvonta on keskeinen osa tietoturvallista IT-ympäristön hallintaa. Puuttuva lokitieto hidastaa vahinkojen selvittämistä, haittaa puhdistustyötä ja vaikeuttaa tuleviin hyökkäyksiin varautumista.*

7. Tietomurtotapauksessa vastuu asian selvittämisestä ja torjumisesta on hyökkäyksen kohteeksi joutuneella organisaatiolla. Kaupunki aloitti tietomurron torjuntatoimet palkkaamansa tietoturvayhtiön kanssa. Torjuntatoimiin ja muihin selvitystoimiin osallistui myös viranomaisia.

   Johtopäätös: *Julkisella sektorilla tietomurtotapausten selvittäminen ja hallinta on riippuvaista yksityisen sektorin toimijoiden asiantuntijuudesta ja saatavuudesta. Toimintamallia yhteistyön käynnistämiseksi, tietojen vaihtamiseksi ja toimenpiteiden koordinoimiseksi ei ole määritelty.*

8. Helsingin kaupunki aloitti sisäisen viestinnän tietomurrosta välittömästi, mutta ulkoisen viestinnän viiveellä. Kaupungin työntekijät tavoitettiin nopeasti henkilökohtaisen viestinnän kautta. Sen sijaan viestinnän kohdentaminen entisille ja nykyisille oppijoille sekä heidän huoltajilleen ja kaupungin muille asiakkaille oli vaikeampaa.

   Johtopäätös: *Tietomurron uhrien tavoittaminen voi olla haasteellista. Yleinen tiedoksianto on tärkeää, mutta se ei yksin riitä varmistamaan viestinnän tavoitettavuutta. Ennakoiva viestintäsuunnittelu ja monikanavainen tiedottaminen on tärkeää, jotta tietomurron uhrit voivat suojautua.*

9. Lapsille ja nuorille kohdennettu tiedottaminen oli puutteellista, eikä se huomioinut riittävästi eri ikä- ja erityisryhmien tarpeita, kuten viestinnän kohdentamista ikätason mukaisesti.

   Johtopäätös: *Alaikäiset tietomurron uhrit eivät välttämättä pysty suojaamaan tietojaan itse. Sen vuoksi viestinnän kohdentaminen lapsille, nuorille ja huoltajille on tärkeää, eikä hankala toteuttaminen saa olla sen esteenä.*

10. Suomessa on mahdollista rajoittaa omien tietojen käyttöä ja luovuttamista julkisissa tietojärjestelmissä. Ne perustuvat henkilön itsensä tekemiin omien tietojen käyttöä rajoittaviin asetuksiin, jotka eivät täysin pysty estämään tietojen käyttöä rikollisiin tarkoituksiin.

    Johtopäätös: *Omien tietojen suojaaminen kattavasti on mahdotonta ja perustuu pitkälti henkilön itse asettamiin rajoituksiin, jotka voivat samalla vaikeuttaa sujuvaa asiointia ja päivittäistä elämää. Tietomurron uhri altistuu pitkäaikaisesti riskille omien tietojen myöhemmästä väärinkäytöstä.*

5 TURVALLISUUSSUOSITUKSET

5.1 Tiedonhallinnan lainsäädännön yhteensovittaminen

Julkisen hallinnon tiedonhallinnassa huomioon otettavia säädöksiä on annettu eri aikoina. Tiedonhallintalakia säädettäessä otettiin huomioon yleisen tietosuoja-asetuksen keskeiset vaatimukset, ja näitä säädöksiä voi pitää keskenään yhteensovitettuina. Tiedonhallintaan liittyvää sääntelyä on edelleen myös muussa lainsäädännössä. Säännöksiä on erityislaeissa ja hallinnon yleislainsäädännössä, kuten arkistolaissa ja julkisuuslaissa. Niitä ei ole kattavasti yhteensovitettu tiedon elinkaaren alusta loppuun ja erityisesti arkistointia koskevat säädökset sekä määräykset ovat vanhoja. Myös teknologiset ratkaisut ovat kehittyneet voimakkaasti, mikä lisää lainsäädännön tarkastamisen tarvetta.

Valvonta- ja ohjaustehtävien jakautuminen useille eri viranomaisille on niin ikään omiaan aiheuttamaan vaikeuksia ohjaavan aineiston yhtenäisyydelle ja niiden soveltajille.

Tutkintaryhmä suosittaa, että

Valtiovarainministeriö yhteistyössä Oikeusministeriön kanssa huolehtii, että julkisen hallinnon tiedonhallintaa koskeva lainsäädäntö yhteensovitetaan ja sen valvonta- ja ohjausrakenteet selkeytetään. [2025-S4]

Säädökset edellyttävät muun muassa päällekkäisiä suunnittelu- ja arviointivelvollisuuksia, kuten tiedonhallintamallin käyttöä, vaikutusten arviointia ja riskien arviointia. Huomiota on kiinnitettävä myös lainsäädännön toimeenpanoon, sen soveltamisen ohjaamiseen ja soveltajien tukemiseen erilaisissa tulkintakysymyksissä. Käytännön soveltamisongelmia ovat aiheuttaneet muun muassa palvelujen tiedonhallinnan toteuttaminen ja pilvipalvelujen käyttö henkilötietojen käsittelyssä.

5.2 Julkisen hallinnon tietoturvapuutteiden havaitsemisen kehittäminen

Julkisen hallinnon tietoturvapuutteiden ennalta havaitseminen on tehokas keino estää haavoittuvuuksien hyväksikäyttöä ja näin ehkäistä tietomurtoja. Tietoverkkorikollisuuden kasvu edellyttää tietoturvallisuustoimenpiteiden kehittämistä laaja-alaisesti ja monikerroksellisesti. Tämä tarkoittaa, että on tärkeää jatkuvasti päivittää ja parantaa tietoturvakäytäntöjä sekä hyödyntää uusimpia teknologioita ja menetelmiä. Lisäksi on olennaista kouluttaa henkilöstöä tietoturva-asioissa ja varmistaa, että kaikki organisaation tasot ovat tietoisia mahdollisista uhkista ja osaavat toimia niiden torjumiseksi. Näin voidaan luoda kattava ja tehokas tietoturvajärjestelmä, joka suojaa julkisen hallinnon tietoja ja resursseja.

Tutkintaryhmä suosittaa, että

Valtionvarainministeriö yhteistyössä Liikenne- ja viestintäministeriön kanssa selvittää millä tavoin julkisen hallinnon tietoturvapuutteiden havaitsemista voidaan valtakunnallisesti parantaa ja varmistaa, että julkisilla toimijoilla on riittävät kyvykkyydet tietoturvapuutteiden havaitsemiseen ja korjaamiseen. [2025-S5]

Nykymuotoinen Hyöky-palvelu ei ole käytössä laajasti julkisen hallinnon toimijoilla. Tarvitaan kuitenkin tietoturvapuutteiden tunnistamiseen tarkoitettu palvelu, joka on helppokäyttöinen ja että sen käyttöönotto on mahdollista kaikille julkisille organisaatioille. Näin voidaan parantaa julkisen hallinnon tietoturvaa kokonaisvaltaisesti.

5.3 Viestinnän ohjeistuksen kehittäminen tietomurtotapahtumissa

Viestintä on osa tietomurtoihin varautumista. Tämä edellyttää ajan tasalla olevaa viestinnän ohjeistusta. Tietomurron tapahtuessa on tärkeää viestiä nopeasti, selkeästi, saavutettavasti ja johdonmukaisesti. Se vähentää epävarmuutta, ehkäisee väärän tiedon leviämistä ja varmistaa, että uhrit saavat tarvitsemansa tuen. Lisäksi on tarjottava ohjeita ja tukea niille, joiden tiedot ovat vaarantuneet. Tietomurroista tiedottamisen on oltava monikanavaista, ikätasolle sopivaa ja kohdennettua sekä saavutettavaa, jotta tieto tavoittaa tietomurron uhriksi joutuneet kattavasti ja ymmärrettävästi. Jos tietomurrosta ei viestitä selkeästi ja johdonmukaisesti, voi syntyä useita riskejä. Epävarmuus lisääntyy, kun asianomaiset eivät tiedä, mitä on tapahtunut ja miten se vaikuttaa heihin, mikä voi aiheuttaa turhaa huolta ja stressiä.

Tutkintaryhmä suosittaa, että

Valtiovarainministeriö yhteistyössä Opetushallituksen kanssa huolehtii, että kunnat ja kaupungit kehittävät tietomurtotapausten viestintään selkeää ja saavutettavaa ohjeistusta, jonka avulla uhrit voivat suojautua tietomurtojen seurauksilta ja suojata omia henkilötietojaan. [2025-S6]

Viestinnän kehittämisessä tulee tavoitella laaja-alaista yhteistyötä erityisesti Opetus- ja kulttuuriministeriön sekä Kyberturvallisuuskeskuksen kanssa. Käytännön toteutuksessa kannattaa hyödyntää nuorten käyttämiä kanavia, kuten sosiaalista mediaa ja viestipalveluita, sekä huoltajille suunnattua tiedotusta journalistisen median, sähköpostin, kirjepostin ja virallisten verkkosivujen kautta. Lisäksi koululuokka on tehokas keino tavoittaa alaikäiset, sillä se mahdollistaa ohjauksen ja kysymysten käsittelyn ikätasolle sopivalla tavalla.

5.4 Kuntien kriittisten tietoturvapuutteiden tunnistaminen ja korjaaminen

Tietoturvan varmistaminen sekä tietomurtojen ennaltaehkäisy edellyttää kunnilta ennakoivia, välittömiä ja jatkuvia toimenpiteitä tietojen käsittelyyn ja tallentamiseen liittyvän riskienhallinnan parantamiseksi.

Tietojen käsittelyyn ja tallentamiseen liittyvien riskien tunnistaminen ja hallinta ovat keskeisiä toimenpiteitä, joilla voidaan varmistaa julkisissa palveluissa tietojen luotettavuus ja tietoturva.

Säännöllinen riskianalyysi auttaa tunnistamaan ja korjaamaan mahdolliset ongelmat ajoissa.

Tutkintaryhmä suosittaa, että

Valtiovarainministeriö yhteistyössä Kuntaliiton kanssa tukee kuntia kriittisten tietoturvapuutteiden tunnistamisessa ja korjaamisessa sekä kehittää tiedonhallinnan ja tietoturvan riskienhallintaa. [2025-S7]

Organisaatioiden tulee tunnistaa, mihin heillä on tallentunut henkilötietoja. Välittömästi tarkasteltavia kohteita ovat organisaation käyttämät tallennuspaikat, kuten esimerkiksi verkkolevyt, chat-palvelut, sähköpostit ja pilvipalvelut. Lisäksi tulee tarkistaa etäyhteyksien tietoturvallisuus.

Kehittämistyössä on hyvä ottaa mukaan hyvinvointialueet ja muut sidosryhmät.

5.5 Toteutetut toimenpiteet

Helsingin kaupungin toimenpideohjelma käynnistettiin tietomurron jälkeen kansliapäällikön päätöksellä, jonka yhteydessä selvitettiin asianhallinnassa ja tietoturvallisuudessa olevat puutteet toimialueittain sekä osoitettiin niihin liittyvät korjaavat toimenpiteet. Toimenpiteet on priorisoitu tärkeyden mukaiseen toteuttamisjärjestykseen. Toimenpiteissä on huomioitu toteutuneen tietomurron mahdollistaneet seikat, esimerkiksi henkilöstön tietoturvallisuuskoulutus, etäyhteyskäytännöt, tietojen tallennuspaikat sekä tietojen poistamisvastuiden määrittelyt. Kehittämisohjelmaan kuuluu säännöllinen raportointivelvollisuus kansliapäällikölle osavuosikatsauksittain.[118]

Helsingin kaupunki teki hankintapäätöksen tietoturvallisuuden lisätoimenpiteistä DigiHelsinki Oy:ltä 12.8.2024. Toimenpiteet liittyvät tietomurrossa havaittujen tietoturvallisuuspuutteiden parantamiseen. Tehdyn lisähankinnan arvo oli 2,6 miljoonaa euroa.[119]

NIS 2-direktiivi on Euroopan unionin kyberturvallisuusdirektiivi, jonka tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa erityisetsi kriittisten sektoreiden osalta. Se asettaa vähimmäistoimenpiteet kyberturvallisuusriskien hallintaan sekä raportointivelvoitteet merkittävissä poikkeamissa. Direktiivi hyväksyttiin marraskuussa 2022, ja sen jäsenvaltioiden on saatettava se osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. NIS 2 direktiiviä täytäntöönpaneva lait annettiin eduskunnalle 23.5.2024 ja ne on hyväksytty eduskunnassa maaliskuussa 2025 ja saatettu voimaan 8.4.2025 lukien. NIS 2 direktiivin mukaista mukaisista velvoitteista julkishallinnolle säädetään julkisen hallinnon tiedonhallinnasta annetun lain uudessa 4 a luvussa. Muiden organisaatioiden osalta velvoitteesta säädetään uudessa kyberturvallisuuslaissa. Lait ovat tulleet voimaan 8.4.2025. Kyberturvallisuuslain [124/2025] mukainen julkishallinnon valvova viranomainen on Liikenne ja viestintävirasto. Lisäksi on huomioitava, että kunnat eivät kuulu kyberturvallisuuslain soveltamisalan piiriin muutoin kuin mahdollisesti harjoittamansa palvelun myötä.

Keväällä 2025 voimaan tullut uusi kyberturvallisuuslaki ja tiedonhallintalain muutokset asettavat uusia velvoitteita myös julkisen sektorin toimijoille. Liikenne- ja viestintävirasto toimii julkisen sektorin toimijoiden valvovana viranomaisena ja pyrkii uudessa roolissaan selkeyttämään sektorin ohjaus- ja valvontarakenteita.

Kriittisten toimijoiden häiriönsietokykydirektiivi (CER, Critical Entities Resilience Directive)[120] astui voimaan 14. joulukuuta 2022, ja jäsenvaltioiden on saatettava sen vaatimukset osaksi kansallista lainsäädäntöään 17. lokakuuta 2024 mennessä. CER-

[118] Kansliapäällikön toimenpideohjelma (Helsingin kaupunki 3.9.2024).
[119] Hankinta, tietoturvan lisätoimenpiteet DigiHelsinki Oy:ltä, kaupunginkanslia. 28.2.2025 https://paatokset.hel.fi/fi/asia/hel-2024-011885?paatos=484a470a-21d9-4e44-a0c2-b4ce754116e1
[120] CER-direktiivi, hallituksen esitys HE 205/2024. 28.2.2025 https://www.finlex.fi/fi/hallituksen-esitykset/2024/205#OT0

direktiivillä tavoitellaan keskinäisriippuvaisten, yhteiskunnan toimintakyvyn kannalta kriittisten palveluiden häiriönsietokyvyn turvaamisen parantamista sekä yhteiskunnan taloudellisten toimintojen ylläpitämistä. CER-direktiivi pantaisiin täytäntöön säätämällä yleislaki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta, jossa säädettäisiin kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevasta kansallisesta strategiasta ja kansallisesta riskiarviosta, toiminnan yleisestä ohjaamisesta ja yhteensovittamisesta, yhteismitallisesta kriittisten toimijoiden arviointikehikosta ja yhtenäisestä kehyksestä kriittisten toimijoiden häiriönsietokyvyn vahvistamiseksi erilaisia uhkia vastaan. Direktiivi tuo uusia tehtäviä yhteensovittavalle ministeriölle, sektoriministeriöille ja viranomaisille. Direktiivin mukaan uusi tehtävä tulee tunnistaa ja määrittää yhdenmukaisin menettelyin kriittiset toimijat sekä valvontaan liittyvät tehtävät. Toimivalta valvoa kriittisiä toimijoita olisi sektorikohtaisilla valvontaviranomaisilla. Kriittisiä toimijoita koskevat keskeiset velvoitteet liittyisivät riskiarviointiin, häiriönsietokykyä koskevaan suunnitelmaan ja häiriönsietokyvyn varmistamiseen sekä poikkeamia koskeviin menettelyihin.

Kyberkestävyyssäädös[121] (CRA, Cyber Resilience Act) (EU) 2024/2847 on Euroopan unionin asetus, jonka tavoitteena on parantaa EU-markkinoilla olevien digitaalisten laitteiden ja ohjelmistojen kyberturvallisuutta vähentämällä niissä esiintyviä haavoittuvuuksia. Säädös asettaa kyberturvallisuuden vähimmäisvaatimukset kaikille laitteille ja ohjelmistoille, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Tämä kattaa esimerkiksi turvakamerat, televisiot, lelut, kotitalousreitittimet, palomuurit sekä erilaiset ohjelmistot, kuten käyttöjärjestelmät ja selaimet.

Valmistajat ovat vastuussa tuotteidensa kyberturvallisuudesta koko niiden elinkaaren ajan. Heidän on varmistettava, että tuotteet on suunniteltu, kehitetty ja valmistettu säädöksen olennaisten kyberturvallisuusvaatimusten mukaisesti. Nämä vaatimukset sisältävät muun muassa turvalliset oletusasetukset, automaattiset turvallisuuspäivitykset, luvattoman pääsyn estämisen sekä datan luottamuksellisen käsittelyn. Lisäksi valmistajien on ilmoitettava selkeästi tuotteidensa tukijakson pituus ja raportoitava aktiivisesti hyödynnetyistä haavoittuvuuksista sekä vakavista tietoturvapoikkeamista Euroopan unionin kyberturvallisuusvirastolle (ENISA) ja kansallisille CSIRT-yksiköille.

[121] Kyberkestävyyssäädös (Cyber Resilience Act, CRA). 28.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra#76938-0

LÄHDELUETTELO

Tutkintaryhmä on saanut kirjallista tutkinta-aineistoa ja tehnyt kuulemisia turvallisuustutkintalain (525/2011) perusteella. Kontaktoituja organisaatioita on 26. Kuulemisten ja alustavien puhuttamisen avulla on saatu tietoja noin 60 ihmiseltä. Tutkintaryhmälle tietoja ovat antaneet organisaatiot ovat:

1. Digi- ja väestötietovirasto
2. DigiHelsinki Oy
3. Dustin Finland Oy
4. Elisa Santa Monica Oy
5. Fujitsu Finland Oy
6. Helsingin kaupunki
7. Helsingin poliisi
8. Helsingin yliopisto
9. Keskusrikospoliisi
10. Kokemusasiantuntijat
11. Kuntaliitto
12. Lapsiasiavaltuutetun toimisto
13. Liikenne- ja viestintäministeriö
14. Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus
15. Maanpuolustuskorkeakoulu
16. Opetus- ja kulttuuriministeriö
17. Opetushallitus
18. Palo Alto Networks
19. Sisäministeriö
20. Suojelupoliisi
21. Telia Cygate
22. Tiedonhallintalautakunta
23. Tietosuojavaltuutetun toimisto
24. Valtion kyberturvallisuusjohtajan toimisto, Liikenne- ja viestintäministeriö
25. Valtiovarainministeriö
26. Rikosuhripäivystys

YHTEENVETO TUTKINTASELOSTUSLUONNOKSESTA SAADUISTA LAUSUNNOISTA

Tutkintaselostusluonnos on ollut lausunnolla valtiovarainministeriössä, liikenne- ja viestintäministeriössä, oikeusministeriössä, opetus- ja kulttuuriministeriössä, sisäministeriössä, Traficomin Kyberturvallisuuskeskuksessa, Opetushallituksessa, Helsingin kaupungilla, Suojelupoliisilla, Keskusrikospoliisilla, Helsingin poliisilaitoksella, Digi- ja viestintävirastossa, Tietosuojavaltuutetun toimistossa, tiedonhallintalautakunnassa, Kuntaliitossa, Lapsiasiavaltuutetun toimistossa, Elisa Santa Monica Oy:ssa sekä Telia-Cygatella.

Yksityishenkilöiden antamia lausuntoja ei turvallisuustutkintalain mukaisesti julkaista.

Valtiovarainministeriö toteaa lausunnossaan, että tutkintaselostus käsittelee poikkeuksellisen hyvin ja seikkaperäisesti Helsingin kaupungin kasvatuksen ja koulutuksen toimialalla tapahtunutta tietomurtoa ja siihen johtaneita syitä. Valtiovarainministeriö toteaa, että tutkintaselostuksessa esitetyt suositukset kohdistuvat lainsäädäntöön ja ohjeistukseen, mutta tutkintaselostuksesta ei kuitenkaan ilmene, että lainsäädännön tila olisi tosiasiallisesti vaikuttanut tietomurtoon. Valtiovarainministeriö esittää, että tutkintaselostuksen suosituksiin lisättäisiin ohjeistusta, jota noudattamalla olisi mahdollista välttää selostuksessa löydettyjä puutteita esimerkiksi palvelunhallinnassa, toimittajahallinnassa ja omaisuudenhallinnassa. Valtiovarainministeriön näkisi myös hyvänä, että tämän tutkintasuosituksen kaltainen tutkimus tehtäisiin kaikista merkittävistä tietomurtotapauksista.

Valtiovarainministeriö toteaa, että tutkintaselvitys ei koske koko kuntasektoria eikä yhden kunnan tapahtumien analysoinnilla ole mahdollista tehdä kaikkiin kuntiin sovellettavissa olevia johtopäätöksiä. Tutkintaselostuksen turvallisuussuositusten osalta valtiovarainministeriö nostaa esille sen, että sen on haasteellista vaikuttaa muiden ministeriöiden vastuulla olevien säädösten valmistelun toteuttamistapaan ja aikatauluun. Tämän vuoksi on ongelmallista, että suosituksessa osassa toimenpiteistä vastuu yhteensovittamisesta asetetaan ensi sijassa valtiovarainministeriölle. Lisäksi valtiovarainministeriö muistuttaa, että tiedonhallintaa koskevaa sääntelyä sisältyy myös muiden ministeriöiden vastuulla oleviin erityislakeihin, joiden valmistelusta vastaa aina kyseisestä sääntelystä vastuussa oleva ministeriö. Valtiovarainministeriö tuo lausunnossaan esiin, että se voi edistää yhteensovittamista eri keinoin, kuten lausunnoin ja ohjeistuksin, mutta viimesijainen vastuu huolehtia yhteensovittamisesta on kulloinkin sääntelystä vastuussa olevalla ministeriöllä.

Valtiovarainministeriö toteaa, että sillä ei ole yleisen kuntien toiminnan ja talouden seurantatehtävän nojalla tiedonsaantioikeutta yksittäisen kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä tai sen riittävyydestä mukaan lukien tietoturvallisuudesta vastaaminen ja puutteiden havaitseminen. Valtiovarainministeriö toteaa, että tilannekuvan muodostaminen yksittäisistä kunnista tai koko kuntasektorin kattavan puutteiden havaitsemisjärjestelmän luominen ei voi siten olla ministeriöiden tehtävä. Lisäksi valtiovarainministeriö tuo lausunnossaan esiin, että kunnat vastaavat itsehallintonsa mukaisesti itse tiedonhallinnan ja tietoturvan sekä viestinnän järjestämisestä kuntalain (410/2015) mukaisesti. Se myös toteaa, että kunta hoitaa itsehallinnon nojalla itselleen ottamansa tehtävät ja järjestää sille laissa erikseen säädetyt tehtävät.

Valtiovarainministeriö korostaa, että tietoturvapuutteiden havaitseminen ja korjaaminen sekä tiedonhallinnan ja tietosuojan riskienhallinnan kehittäminen ovat osa kunnan sisäistä valvontaa ja riskienhallintaa ja siten kunkin kunnan kunnanhallituksen vastuulla. Valtiova-

rainministeriö myös toteaa, että ministeriöillä ei voi olla vastuuta tiedonhallinnan ja tietosuojan riskienhallinnan kehittämisestä tai esimerkiksi riittävien kyvykkyyksien varmistamisesta kaikissa kunnissa. Sama koskee myös viestinnän riittävyyden varmistamista.

Valtiovarainministeriön näkemyksen mukaan kuntien omaa vastuuta tiedonhallinnan järjestämisestä ei tule ohittaa yksinomaan sillä perusteella, että turvallisuussuosituksen toteutumisen seurannan kannalta suositus on helpompaa kohdistaa ministeriöihin. Valtiovarainministeriö tuo myös esiin, että nyt suosituksia ei ole kohdistettu lainkaan kunnille tai kuntien tilintarkastukseen. Valtiovarainministeriö toteaa, että tarpeet tietoturvapuutteiden tunnistamiseen ja korjaamiseen voivat vaihdella organisaatiokohtaisesti ja siksi ne ovat kunkin organisaation omalla vastuulla. Valtiovarainministeriön mukaan kuntia koskevat suosituksen voisivat olla tarpeen myös hyvinvointialueille.

Liikenne- ja viestintäministeriön lausunnon mukaan tutkintaselostus kuvaa selkeästi tilanteen etenemistä, sen aikaisia tapahtumia ja niiden aikana tehtyjä toimia. Tutkintaselostus avaa tapaukseen johtaneita tekijöitä ja tapahtuman seurauksia siten, että muut organisaatiot voivat hyödyntää tutkinnan havaintoja oman toimintansa kehittämisessä turvallisempaan suuntaan ja ehkäistä siten uusia vahinkoja.

Lisäksi liikenne ja viestintäministeriö toteaa, että kyberturvallisuuden tasoon vaikuttaa merkittävästi myös eri organisaatioiden kyberturvallisuuteen käyttämät resurssit, minkä lisäksi viranomaisten toiminnan ja palvelujen kehittäminen edellyttää resursointia. Tutkintaselostuksessa kiristyneen valtiontalouden merkitystä erityisesti julkishallintoon ja sen myötä tuotettavien kyberturvallisuuspalveluihin ei ole nostettu esiin. Liikenne- ja viestintäministeriö korostaa, että tietoturva puutteiden havaitseminen ja muut kyberturvallisuuden parantamiseksi tuotettavat palvelut edellyttävät jatkuvaa resursointia.

Liikenne- ja viestintäministeriö toteaa, että suositukset nykyisellään kohdistuvat pääasiassa ministeriöille ja jotta samankaltaiset onnettomuudet ja vaaratilanteet voidaan jatkossa välttää niin kunnissa, yrityksissä ja muissa organisaatioissa, suosituksia tulisi harkita kohdistettavan ennakollisen varautumisen vahvistamiseksi myös niille.

Liikenne ja viestintävirasto tuo esiin, että Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tuottamien palveluiden jatkuvuuden varmistaminen ja palveluiden, kuten Kybermittarin ja Hyökyn käytön laajentaminen laajemmille kohderyhmille sekä HAVARO-palvelun toiminnan ja jatkuvuuden turvaaminen on huomioitu myös Suomen kyberturvallisuusstrategiassa 2025–2035 ja sen toimeenpanosuunnitelmassa, mutta näiden toimenpiteiden on kuitenkin todettu myös strategiassa edellyttävän lisäresursseja.

Liikenne- ja viestintäministeriö nostaa lausunnossa esille, että Helsingin kaupungin tietomurtoa koskevan tutkinnan aikana saatuja kokemuksia sekä valmistunutta tutkintaselostus on tärkeää hyödyntää lainvalmistelun tukena ja hallitusohjelma kirjauksen huomioimiseksi. Lain valmistelussa tulee pohtia eri vaihtoehtoja kyberturvallisuuteen. Kohdistuneiden vakavien häiriöiden turvallisuustutkinnan toteuttamiseksi huomioiden myös se, että jo nykyisellääkin voidaan tehdä poikkeuksellisen tapahtuman tutkintaa.

Opetus ja kulttuuriministeriö toteaa lausunnossaan, että tutkintaselostus on hyvin ja seikkaperäisesti laadittu. Selostus sisältää olennaista ja arvokasta tietoa Helsingin kaupunkiin kohdistuneen tietomurron syistä, vaikutuksista ja poikkeamanhallinnan menettelyistä. Opetus- ja kulttuuriministeriön mukaan selostus sisältää myös organisaatioille arvokkaita oppeja kyberturvallisuuden kehittämisestä, riskienhallinnasta ja poikkeamatilanteiden hallinnasta. Sisältö auttaa osaltaan myös opetus- ja kulttuuriministeriön hallinnonalan mahdollisten jatkotoimenpiteiden suunnittelussa.

Opetus- ja kulttuuriministeriö toteaa, että ministeriön substanssin näkökulmasta tutkintaselostuksen luonnos ei sisällä sellaista eksplisiittistä tietoa, joka vaarantaisi turvajärjestelyiden toteutumisen, tai ei sopisi muutoin julkiseen asiakirjaan. Opetus- ja kulttuuriministeriö kuitenkin toteaa, että tutkintaselostus sisältää hyvin yksityiskohtaisia kuvauksia ja joka voi aiheuttaa Helsingin kaupungille lisää merkittävääkin mainehaittaa sekä vaikuttaa siihen, kuinka kohdennetusti Helsingin kaupunki jatkossa joutuu tai valikoituu erilaisten kyberhyökkäysten kohteeksi. Opetus- ja kulttuuriministeriön näkemyksen mukaan julkisessa versiossa dokumentti voisi sisältää yleisemmän ja lyhyemmän kuvauksen tai yhteenvedon tapahtumien kulusta ja onnistuneeseen tietomurtoon johtaneista tekijöistä.

Opetus- ja kulttuuriministeriö toteaa suositusten kohtaan 5.1, että esitetyn ohella käytännön soveltamisongelmia voi olla tilanteissa, joissa henkilötietoja käsitellään eri hallinnonalojen välillä. Esimerkkinä opiskeluhuollon palvelut, jossa käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja sekä hyvinvointialueiden että opetustoimen lakisääteisten tehtävien toteuttamisessa. Laki oppilas- ja opiskelijahuoltolain muuttamisesta (377/2022) on luonut vaihtelevia tulkinta- ja toteutuskäytäntöjä, mutta myös tehnyt opetustoimen tietoturva- ja tiedonhallintaympäristön monimutkaisemmaksi.

Suositusten kohta 5.3 opetus- ja kulttuuriministeriö toteaa, että ehdotus laaja-alaisemmasta yhteistyöstä erityisesti opetus- ja kulttuuriministeriön sekä Kyberturvallisuuskeskuksen kanssa on kannatettava. Vastaavaa yhteistyötä on mahdollista tehdä myös sellaisten toimenpiteiden osalta, joiden tavoitteena on ennaltaehkäistä tietomurtoja, tai edistää niihin varautumista. Selkeät vastuut sekä viestinnän ja raportoinnin toimintatavat ovat olennainen osa toimivan poikkihallinnollisen tilannekuvan muodostamista sekä poikkeamienhallintaa.

Liikenne- ja viestintävirasto Traficomin on jäsentänyt lausuntonsa neljään kokonaisuuteen, jotka ovat Traficomin Kyberturvallisuuskeskuksen lakisääteiset tehtävät, Kyberturvallisuuskeskuksen toimenpiteet tapauksessa, Kyberturvallisuuskeskuksen kyberpalvelut sekä kommentit johtopäätöksistä ja turvallisuussuosituksista.

Traficom huomauttaa, että sen kyberturvallisuuteen liittyvät lakisääteiset tehtävät on kuvattu vain osittain tutkintaselostusluonnoksessa, ja se avaa lausunnossaan tarkemmin lakisääteisiä tehtäviä sekä Traficomin ja muiden viranomaisten keskinäistä toimintaa sekä yhteistyötä erilaisissa kyberpoikkeamatilanteissa. Lisäksi Traficom nostaa esille, että tietoturvaloukkauksia tutkivien viranomaisten keskinäinen yhteistyö tietoturvaloukkaustilanteissa on toimivaa ja rutinoitunutta, mutta tätä yhteistyötä tulisi edelleen kehittää ja harjoitella.

Lausunnossaan Traficom korostaa, että Kyberturvallisuuskeskuksen operatiivisten kyberturvallisuustehtävien lisäksi tutkintaselostuksessa olisi syytä huomioida myös kyberturvallisuuteen liittyvät valvontatehtävät, jotka löytyvät Sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 303.1 §:stä. Tämän ohella Traficom nostaa esille, että se toimii valvovana viranomaisena NIS2-/kyberturvallisuusdirektiiviin perustuvan kansallisen kyberturvallisuuslain 26 §:n 1 momentin 1 kohdan ja tiedonhallintalain 18 h §:n mukaisesti usealla toimialalla.

Traficom myös toteaa, että tutkintaselostus antaa virheellisen kuvan tietyistä Kyberturvallisuuskeskuksen julkiselle sektorille tarjoamista kyberturvallisuuspalveluista, joita he tarkentavat lausunnossaan.

Traficom tuo esiin esitettyihin johtopäätöksiin liittyen, että valvovan viranomaisen tehtävissä korostuvat sekä ennakolliset ohjaavat toimenpiteet sekä jälkikäteen toteuttava valvonta. Ennakollisella ohjauksella on parhaimmat mahdollisuudet tavoittaa käytössä olevilla valvovan viranomaisen resursseilla valvonnan kohteena olevat organisaatiot. Ennakollinen ohjaus on

Traficomin näkemyksen mukaan tehokas valvontakeino kyberturvallisuuden saralla. Valvonnan ohjaavat toimenpiteet eivät kuitenkaan pois sulje muiden valvontatyökalujen hyödyntämistä. Traficom toteaa, että jos valvovilla viranomaisilla olisi nykytilanteeseen verrattuna moninkertaiset resurssit, niin tällöin voitaisiin pohtia eri sektoreilla perustavanlaatuisia muutoksia myös jälkikäteiseen valvontaan ja esimerkiksi valvonnan kohteena oleviin organisaatioihin kohdistuvaan tarkastustoimintaan. Kyberturvallisuuden valvonta- ja ohjaustehtävät ovat pääsääntöisesti resursoitu hyvin niukasti eri viranomaisissa Suomessa.

Traficom yhtyy lausunnossaan näkemykseen siitä, että myös julkisen sektorin kyberturvallisuutta ja kykyä vastata eri tietoverkkorikosten uhkiin tulee kehittää tulevina vuosina. Tämä edellyttää Traficomin mukaan erityisesti kyberturvallisuutta kehittävien toimien ja henkilöstön resursointia, koulutusta ja tarvittavien teknisten menetelmien hyödyntämistä. Traficomin arvion mukaan julkisen sektorin kykyyn vastata vakaviin valtiollisiin uhkiin, mutta myös tietoverkkorikollisten aiheuttamiin uhkiin voisi olla syytä panostaa merkittävästi. Traficomin mukaan tämä voisi esimerkiksi pitää sisällään erityisiä panostuksia hyökkäysten ja haavoittuvuuksien havainnointi- ja reagointimenetelmiin, kuten Kyberturvallisuuskeskuksen HAVARO- ja Hyöky-palveluihin.

Traficomin mukaan myös julkisella sektorilla organisaatiolla itsellään on viime kädessä vastuu oman tietoturvan ja kyberturvallisuuden ylläpitämisestä ja kehittämisestä. Traficom korostaa, että myös julkisella sektorilla käytössä olevia kyberturvallisuutta koskevia prosesseja ja menetelmiä tulee tarkastella uudestaan uuden kyberturvallisuuslain ja tiedonhallintalakiin tehtyjen muutosten myötä.

Traficom muistuttaa, että voimaan tullut uusi kyberturvallisuuslaki ja tiedonhallintalain muutokset asettavat uusia velvoitteita myös julkisen sektorin toimijoille.

Traficom kannattaa ehdotettua turvallisuussuositusta (suositus 5.2.), sillä Suomen kansallisen kyberturvallisuuden parantamisen näkökulmasta julkisen hallinnon tietoturvapuutteiden havaitsemisen kehittämistä voidaan pitää keskeisenä toimenpiteenä kyberturvallisemman Suomen puolesta.

Opetushallitus tarkentaa lausunnossaan tietoja julkaisemistaan oppaista ja ohjeista. Opetushallitus korostaa, että sillä ei ole toimivaltaa linjata tietosuojalainsäädännön tulkinnasta, joten sen oppaiden ja tukimateriaalien laajuus riippuu saatavilla olevasta oikeuskäytännöstä sekä valvontaviranomaisten ratkaisuista. Opetushallitus esittää, että Opetushallituksen rooli muotoiltaisiin suosituksessa vastaamaan viraston tehtävää esimerkiksi niin, että Opetushallitus tukee kasvatuksen, opetuksen ja koulutuksen järjestäjiä kehittämään selkeää ja saavutettavaa ohjeistusta viestinnässä tietomurtotapauksiin liittyen.

Digi- ja väestötietovirasto toteaa lausunnossaan, että tietoturvallisuuden ylläpitoon on nykyisellään riittävästi säädöksiä ja asiaa koskeva peruslainsäädäntö on kunnossa. Heidän mukaansa haasteet ovat säädösten tuntemisessa ja resursseissa täyttää vaatimukset täysimääräisesti. Digi- ja väestötietoviraston mukaan olisi tärkeämpää tukea ja ohjata toimijoita säädösten vaatimusten täyttämisessä kuin lisätä valvontaa.

Tietosuojavaltuutettu kiinnittää lausunnossaan huomiota eräiden käsitteiden käytön ja oikeudellisten yksityiskohtien täsmällisyyteen ja pyytää tarkentamaan niitä. Lausunnossa tuodaan esille, että selosteesta eivät käy ilmi kaikki tietosuojavaltuutetun toimiston tapauksessa toteuttamat toimenpiteet. Tietosuojavaltuutetun toimisto kiinnittää huomioita myös siihen, että tietosuojavaltuutettu toteuttaa säännönmukaista valvontatoimintaa, mutta sen nykyistä painokkaampi toteuttaminen edellyttäisi toimiston parempaa resurssointia.

Lapsiasiavaltuutettu toteaa lausunnossaan, että tutkintaselostus on selkeä ja yksityiskohtainen ja siitä saa erinomaisesti kuvan tapahtuneesta tietomurrosta, sen selvittelystä, viestinnästä sekä johtopäätöksistä ja suosituksista. Lapsiasiavaltuutetun mukaan tutkintaselosteessa on hyvin tunnistettu tarve viestiä lapsille ja nuorille ikätasoisesti tietomurrosta ja sen seurauksilta suojautumisesta sekä omien henkilötietojen suojaamisesta. Lapsiasiavaltuutettu tarkentaa, että Suomessa Tietosuojalain (1050/2018) 5 §:n mukaan tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettava ikäraja on vähintään 13 vuotta.

Helsingin kaupunki pitää lausunnossaan tietomurron tapahtumien selvittämistä ja siitä tehtäviä johtopäätöksiä hyödyllisenä, sillä tietoja voidaan käyttää jatkossa tietoturvan, tiedonhallinnan ja tietosuojan kehittämisen tukena. Helsingin kaupunki katsoo, että tutkintaselostus on ansiokkaasti laadittu ja kattava selostus tapahtuneesta.

Helsingin kaupungin näkemyksen mukaan tietomurto oli ammattimainen, hyvin suunniteltu ja tehokkaasti toteutettu. Helsingin kaupunki arvioi sen kohteeksi joutuneiden uhrien määräksi noin 150 000 oppijaa huoltajineen sekä kaikki 38 000 kaupungin työntekijää.

Lausunnossaan Helsingin kaupunki perustelee valitsemaansa tiedotuslinjaa. Alkuvaiheessa henkilökohtainen tiedottaminen kaikille rekisteröidyille arvioitiin mahdottomaksi, joten tiedotuksessa turvauduttiin tietosuoja-asetuksen mahdollistamaan yleiseen tiedoksiantoon. Helsingin kaupunki ilmoitti ratkaisustaan tietosuojavaltuutetulle ja toimitti tälle tietoja tehdyistä informointitoimenpiteistä. Helsingin kaupunki korostaa, että se arvioi henkilökohtaisen tiedottamisen toteutusmahdollisuuksia säännöllisesti tietomurron ja sen jälkiselvittelyjen aikana, mutta koska vuotaneet tiedot eivät selvinneet riittävällä tarkkuudella, ei henkilökohtaiselle tiedottamiselle katsottu syntyneen riittäviä edellytyksiä. Tietosuojavaltuutettu ei myöskään ohjeistanut toimimaan toisin.

Helsingin kaupunki toteaa, että ottaen huomioon tutkinnan keskeneräisyyden kaupunki katsoo, ettei ulkoista viestintää olisi voitu toteuttaa nopeammassa aikataulussa. Helsingin kaupunki tuo lausunnossaan esiin näkemyksen, että verkkolevyn vanhentuneiden tiedostojen poistoihin liittyen käytännössä ohjeita oli annettu, mutta niiden noudattamista ei valvottu.

Helsingin kaupungin mukaan pistemäisten säädösten lisäksi kunnan eri toimivaltaisille viranhaltijoille jaettu toimivalta pirstaloittaa palvelujen vaatimien tietojärjestelmien hankintaa ja kehittämistä. Nykyaikaisen ja tietoturvallisen ICT-arkkitehtuurin johtaminen edellyttää tekniikkaan ja ydintietojärjestelmiin liittyvän päätöksenteon keskittämistä. Tämänkin vuoksi tiedonhallinnasta vastaavien on vaikea hahmottaa vaatimusten kokonaisuutta, mikä johtaa näiden vaihtelevaan soveltamiseen.

Helsingin kaupunki pitää annettuja suosituksia tarpeellisina, joskin melko laajoina, mikä voi tehdä niiden toteuttamisesta ja hallinnasta vaativaa. Helsingin kaupunki pitää perusteltuna tavoitetta kehittää tietoturvapuutteiden ennakollista havaitsemista ja korjaamista.

Helsingin kaupunki katsoo viestinnän ohjeistuksen kehittämistä koskevan kohdan olevan ongelmallinen, sillä kunnan viestinnän kehittäminen kuuluu perustuslain 121. pykälän mukaan kuntien itsensä vastuulle. Viranomaiset voivat tukea kunnan tehtävää mutta eivät huolehtia siitä. Kuntaliiton tukea tietoturvapuutteiden tunnistamisessa ja korjaamisessa sekä tiedonhallinnan ja tietosuojan kehittämisessä kaupunki pitää erittäin hyvänä ajatuksena.

Helsingin kaupunki muistuttaa koulujen tietoturvaan liittyen, että oppilaita on paljon ja peruskoulussa he ovat vielä alaikäisiä, mikä muodostaa merkittävän haasteen kouluympäristöjen tietoturvalle varsinkin suuremmissa kunnissa. Kaupungin näkemyksen mukaan tutkintaraportissa ei ole riittävästi huomioitu sitä näkökulmaa, että oppilaiden ja opiskelijoiden tietoturvataitojen kehittäminen ei ole ainoastaan opetussuunnitelman tavoitteiden toteuttamista

vaan myös organisaation omien järjestelmien tietoturvan ylläpitämistä. Helsingin kaupunki toteaa, että Opetushallituksen tulisi huomioida lasten digiosaamisen kehittäminen opetussuunnitelmassa sekä laadittava ohjeistusta siitä, miten tietoturva huomioidaan tilanteissa, joissa oppilaiden heikot digitaidot aiheuttavat riskin ympäristölle.

Helsingin kaupunki toteaa laajaan tietomurtoon liittyvien vahingonkorvauskysymysten olevan merkittäviä, sillä suoran vahingon lisäksi myös perusteltu pelko henkilötietojen mahdollisesta vuotamisesta tai tulevasta väärinkäytöstä voi oikeuttaa korvauksiin. Aineeton vahinko on korvattavuudeltaan yhtä arvokas kuin aineellinen vahinko. Siksi pienikin tietoturvapuute tai laiminlyönti voi johtaa laajakantoisiin ja kalliisiin vahinkoihin. On tärkeää, että vahingot korvataan lain nojalla perustuen syy-yhteyteen ja näytettyyn vahinkoon niin, ettei sääntelystä tai korvauskäytännöistä muodostu ylivoimaisia.

Helsingin kaupunki esittää lausunnossaan lisäksi pieniä täsmennyksiä tapahtumien kulkuun sekä yksityiskohtiin.

DigiHelsinki Oy toteaa lausunnossaan, että se on tuottanut palomuuripalveluita puitesopimuksen palvelukuvauksen mukaisesti eikä palvelu sisältänyt tietoturvahälytysten valvontaa. Lausunnon mukaan tietomurrossa käytetty ASA 5515 ei missään vaiheessa ollut DigiHelsingin hallinnassa eikä yhtiöllä ollut näkyvyyttä laitteeseen tai KASKOn sisäverkkoon. DigiHelsinki oli kilpailuttanut tietoliikennelaitteiden asennuspalvelun ja välitti sen mukaisesti KASKOn tilaaman varmenteen päivitystehtävän Dustin Oy:n toteutettavaksi. DigiHelsingin näkemyksen mukaan ASA 5515:n omistajuus ja ylläpito ovat kuuluneet KASKOlle. Lisäksi DigiHelsingin lausunnossa esitetään tarkennuksia liittyen haittaohjelmien torjuntaohjelman hälytysten ja tikettien käsittelyyn.

Kuntaliitto pitää lausunnossaan hyödyllisenä, että Helsingin kaupungin tietomurron kulku on selvitetty ja että sen yhteydessä on tunnistettu turvallisuussuositukset vastaavien tapahtumien ehkäisemiseksi. Erityisen ansiokkaana Kuntaliitto pitää raportin yksityiskohtaista kuvausta tietomurron etenemisestä ja syistä onnistuneen tietomurron takana. Kuvausta voidaan Kuntaliiton mukaan hyödyntää kuntien tietoturvan ja tietosuojan kehittämisen tukena. Kuntaliitto esittää, että kuvauksen pohjalta voisi määritellä suoraan yksityiskohtaisen kehittämiskohteiden listan kullekin organisaatiolle.

Kuntaliitto pitää tärkeinä raporttiluonnokseen kirjattuja suosituksia. Suositukset nähdään kuitenkin monelta osin laajoiksi ja yleisiksi, jolloin niiden toteuttamiskelpoisuutta pidetään kyseenalaisena. Kuntaliitto korostaa lausunnossaan hyvän tiedonhallinnan merkitystä sille, että tietosuojaan ja tietoturvaan liittyvät toimenpiteet toimivat tehokkaasti ja kohdentuvat oikeisiin asioihin. Se toteaa, että lainsäädäntöä ja erilaista ohjeistusta on paljon, mutta ne ovat hajallaan ja kunnat saavat soveltamiseen hyvin vähän tukea suoraan viranomaisilta.

Kuntaliiton näkemyksen mukaan tulisi pohtia, miltä osin viimeaikainen ymmärryksen lisääntyminen kuntien roolista osana kansallista varautumista sekä kuntien henkilötietovarantojen kriittisyydestä tulisi näkyä kansallisissa kyberturvallisuuden strategioissa, toimintasuunnitelmissa ja rahoituspäätöksissä. Kuntaliiton näkemyksen mukaan tiedonhallinnan nykytilanne ei ole välttämättä niin ongelmallinen kuin mitä raportti antaa ymmärtää.

Kuntaliitto tuo esille, että tiedonhallintalain 4. luvun eli tietoturvavaatimusten toteutumista ei arvioi mikään taho. Kuntaliitto pitää tärkeänä saada ratkottua em. lainsäädännön ja sen toimeenpanon ongelma, jotta tiedonhallintalain 4. luvun toteutumisen arvioinnin toteuttaminen saataisiin käynnistettyä ja toteutettua pitkäjänteisesti.

Keskusrikospoliisi esittää tutkintaselostukseen omaa organisaatiotaan koskevan teknisen korjauksen. Muilta osin sillä ei ollut lausuttavaa.

Oikeusministeriöllä ei ollut tutkintaselostuksesta lausuttavaa.