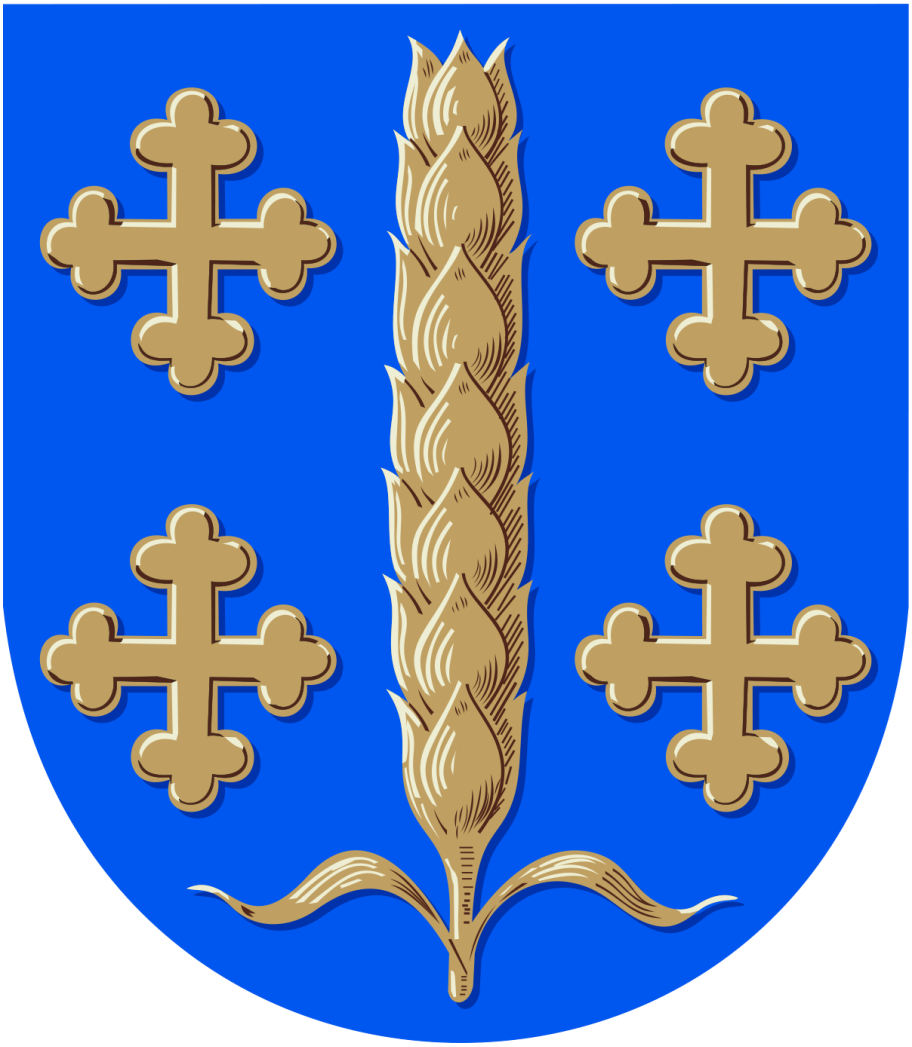
TIETOTILINPÄÄTÖS 2020



Jari Kipinoinen, tietosuojavastaava

jari.kipinoinen@loimaa.fi

Sisällys

TAUSTAA

Tietotilinpäätös

Loimaan tietotilinpäätöksessä kuvataan tietosuojan ja -turvan tilannetta vuonna 2020. Tilinpäätökseen on koottu toimenpiteitä tietoturvan toteuttamisesta käytännössä ja mitä uusia toimenpiteitä on otettu käyttöön kuluvana vuonna. Lisäksi käydään läpi, onko mahdollisia tietoturvaloukkauksia tapahtunut ja mitä toimenpiteitä nämä ovat aiheuttaneet.

Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, niitä luovutetaan eteenpäin ilman lupaa tai niihin pääsee käsiksi taho, jolla ei ole oikeutta kyseisiin tietoihin.

Esimerkkejä tietoturvaloukkauksista ovat esimerkiksi

- Toisen henkilön potilastietojen tarkastelu ilman hoitosuhdetta
- Kadonnut muistitikku, joka sisältää henkilötietoja tms. arkaluontoista tietoa
- Hakkerointi
- Haittaohjelmatartunta

Tietoturvaloukkauksiin on kyettävä reagoimaan nopeasti ja tämän vuoksi onkin laadittava toimintaohjeet mahdollisia tietoturvaloukkaustilanteita varten.

Rekisterinpitäjän tulee arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu, esimerkiksi

- Ei riskiä
- Aiheutuu riski
- Aiheutuu korkea riski

Toimenpiteet tietoturvaloukkauksen jälkeen riippuvat riskin tasosta, mutta kaikki loukkaukset tulee dokumentoida.

Mikäli tietoturvaloukkauksesta aiheutuu riski luonnollisten henkilöiden oikeuksille ja vapauksille, tulee tietosuojavaltuutetun toimistoon tehdä ilmoitus 72 tunnin kuluessa. Ilmoitus tehdään sähköisellä lomakkeella (https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta). (https://tietosuoja.fi/tietoturvaloukkaukset)

TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Loimaan kaupungille on laadittu tietoturvapolitiikka. Tiedon turvaaminen on tärkeä osa kaupungin toiminnan ja sen järjestämien palvelujen laatua. Tietoturvan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää. Tietoturvapolitiikka määrittelee Loimaan kaupungin tietoturvan tavoitteet, vastuut, tietoturvatyön organisoinnin ja toteutuskeinot. Se kuvaa myös seurannan ja tiedottamisen yleisperiaatteet.

Henkilöstölle on laadittu tietoturvaohje, joka löytyy verkkolevyltä (L:\tietopankki\Tietohuolto\Tietoturvatyöryhmä\dokumentit\Henkilöstön tietoturvaohje.pdf). Ohjeessa otetaan kantaa mm. toimitilaturvallisuuteen sekä tunnuksiin ja salasanoihin. Tietoturvaohje päivitettiin vuonna 2020.

Varhaiskasvatuksen ja perusopetuksen henkilöstölle on laadittu erillinen tietosuojaohje.

Käyttäjiä on aiemmin ohjeistettu tekemään Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) toteuttama Arjen tietosuojan nettitestin (https://arjentietosuoja.fi/fi/#/quiz). Tämän ohjeistuksen noudattamista tulee jatkaa myös uusien työntekijöiden kohdalla.

Johtoryhmä osallistui Taisto2020-koulutukseen 19.11.2020.

Tietosuojaselosteet löytyvät kaupungin kotisivuilta.

Salatun sähköpostin lähetys on ollut käytössä jo useamman vuoden. Kaupungin sisällä liikkuva posti (loimaa.fi -> loimaa.fi) on aina salattua, mutta ulkopuolisille tahoille lähettävä sähköposti, joka sisältää arkaluonteista tietoa, tulee salata F-Securen suojausratkaisulla. Ohje salaukseen löytyy verkkolevyltä, johon kaikilla on pääsy. (L:\tietopankki\Tietohuolto\ATK-oppaat ja ohjeet\sähköposti\Salatun sähköpostin lähettäminen.pdf)

Kaupungissa on käytössä suurissa monitoimilaitteissa turvatulostus. Tulostettaessa työasemalta monitoimilaitteelle, pitää käyttäjän mennä fyysisesti laitteen luokse ja heilauttaa kulkuläpyskäänsä lukijan luona. Vasta tämän jälkeen tulostustyö tulostuu paperille. Sote-puolella turvatulostuksen käyttöä ollaan suunnittelemassa kaupungin leasing-laitteiden vaihtuessa 2m-it:n toimittamiin monitoimilaitteisiin.

Arkaluonteiset tiedostot tallennetaan omalle verkkolevylle, jossa pääsyoikeuksia on jaettu kansiokohtaisesti. Lisäksi tiedostojen käytöstä muodostuu käyttöloki.

Vuonna 2020 käyttöön otettuja uusia toimenpiteitä tietoturvan lisäämiseen

26.2.2020 tapahtuneen onnistuneen tietojenkalastelun myötä kaksivaiheisen tunnistuksen käyttöönottoa laajennettiin esimiehiin. Tulevaisuudessa tarkoitus on laajentaa kaksivaiheinen tunnistautuminen koskemaan kaikkia kaupungin työntekijöitä. Ongelmaksi tosin muodostuu henkilökohtaisten puhelinten puute esim. hoitohenkilökunnalla.

Loimaan kaupungin sähköpostien siirtoa Microsoftin pilveen (Office 365) jatkettiin. Suunnitelmana oli, että kaikki työntekijät käyttäisivät Microsoftin pilvipalveluita vuoden 2020 loppuun mennessä.

Puhelinten hallintaohjelman (Intune) käyttöönottoa on jatkettu. Hallintaohjelman avulla puhelimiin vaaditaan asetettavaksi lukituskoodi. Mikäli puhelin katoaa, voidaan laite tarvittaessa tyhjentää etänä. Lisäksi ohjelmien omatoimista asennusta/asentumista voidaan rajoittaa.

Kaupungin eri yksiköitä siirtyi Ylistaronkatu 36:n kiinteistöön vuoden 2020 aikana. Liikkumista kiinteistössä on rajoitettu – vain yksi ulko-ovista on virka-aikana auki ja väliovista kulkeminen tapahtuu kulkuläpyskällä. Näin estetään epämääräisten henkilöiden vapaa liikkuminen kiinteistössä. Kyseisen kiinteistön neuvottelutiloja ei myöskään tällä hetkellä vuokrata ulkopuolisille.

SEURANTA JA TIETOTURVALOUKKAUKSET

Sosiaali- ja terveyspalvelut

Sosiaali- ja terveyspalveluissa suoritetaan joka vuosi pistokokeita, joissa selvitetään satunnaisesti valittujen käyttäjien toiminta potilastietoja sisältävissä ohjelmissa (Pegasos, Winhit, Pro Consona). Vuonna 2020 valvontapäiviä oli yhteensä neljä. Tarkistuksissa ei havaittu väärinkäytöksiä.

1. Avoimen työpaikan hakijoiden tietoja päätynyt vääriin osoitteisiin

Tietosuojavastaavalle ilmoitettiin 14.9.2020 tilanteesta, jossa avoinna olevan työpaikan hakijoille lähetettiin vahingossa kaikkien hakijoiden hakemukset (sisälsivät nimitiedot, osoitetiedot, puhelinnumerot, mutta ei henkilötunnuksia). Kaikille hakijoille ilmoitettiin asiasta. Sosiaali- ja terveyspuolen tietosuojavastaava teki ilmoituksen tietosuojavaltuutetun toimistoon.

2. Työntekijöiden henkilötunnukset näkyvissä asiakastietojärjestelmän asiakirjaselauksessa

Tietosuojavastaava sai tietoonsa 5.11.2020, että asiakastietojärjestelmän asiakirjaselauksesta näkyvät Loimaan kaupungin ko. ohjelman käyttäjien henkilötunnukset asiakkaiden eri palvelutapahtumien kohdalla. Asiasta ilmoitettiin ohjelmiston toimittajalle ja tietosuojavaltuutetun toimistoon samana päivänä.

Tietosuojayhteyshenkilö teki yhdessä kaupungin tietosuojavastaavan kanssa 6.11.2020 ilmoituksen tietosuojavaltuutetun toimistoon. Lisäksi kaupungin tietosuojavastaava ilmoitti asiasta ohjelmistotoimittajan tietosuojavastaavalle ja yhteyshenkilölle. Myös asianomaiselle valvontaviranomaiselle tehtiin ilmoitus.

Ohjelmiston toimittaja ilmoitti sähköpostitse käynnistävänsä asianmukaiset prosessit tilanteen selvittämiseksi ja korjaamiseksi välittömästi, korkeimmalla prioriteetilla.

Henkilöstöä tiedotettiin asiasta 6.11.2020. Samalla muistutettiin, että työntekijällä ja viranhaltijalla on salassapitovelvollisuus kaikkeen henkilöön kohdistuvaan tietoon eikä tämä järjestelmävirhe vapauta ketään omasta henkilökohtaisesta vastuusta saadessaan käsiinsä salassa pidettävää tietoa.

Ratkaisuna ongelmaan ohjelmiston toimittaja muokkasi ohjelman käyttöoikeuksia siten, että vastaava ongelma ei enää ole mahdollinen.

Asiasta tehtiin riskiarvio ja todettiin, että salassa pidettäviä tietoja ei ole päässyt julkisuuteen. Näin ollen tietosuojaloukkausta pidetään vähäisenä.

Kaupungin muut palvelut

1. Office 365 -tunnuksen ja salasanan onnistunut kalastelu (phishing)

Loimaan kaupungin työntekijän sähköpostin salasana onnistuttiin 26.2.2020 selvittämään tietojenkalastelun avulla. Tiliä käytettiin uusien kalasteluviestien lähettämiseen. Lisäksi työntekijän sähköpostiin luotiin sääntö, jolla saapuneet viestit ohjattiin automaattisesti toiseen kansioon. Näin työntekijää estettiin saamasta varoitusviestejä kalasteluyrityksen kohteilta.

Työntekijän sähköpostitili suljettiin ja kaappaajan luoma sääntö saapuvien viestien siirrosta purettiin. Tietosuojavaltuutetun toimistoon tehtiin ilmoitus ja heille lähetettiin lokitietoja sekä esimerkki kalasteluviestistä. Eniten kalasteluviestejä saaneiden yritysten/kuntien/viranomaisten tietosuojavastaaville lähettiin varoitus ja toimitettiin pyydettäessä listaus osoitteista, joihin viestejä oli lähetetty.

Asiasta tehtiin riskiarvio ja todettiin tietosuojaloukkauksen olevan laaja, mutta vaikutuksiltaan vähäinen.

2. Microsoftin teknisen tuen huijauspuhelut

Kaupungin puhelimiin on tullut puheluita, joissa soittaja esiintyy englantia puhuvana Microsoftin tukihenkilönä. Soittajan tarkoituksena on saada käyttäjä asentamaan etähallintaohjelmisto tietokoneelle. Käyttäjiä on ohjeistettu sulkemaan puhelu. Huijauspuhelut eivät ole aiheuttaneet tietomurtoja Loimaan kaupungissa.

3. Loimaan kaupungin työntekijöiden palkka-aineiston toimittaminen väärään sähköpostiosoitteeseen

Ohjelmistotoimittaja toimitti vuonna 2020 Loimaan kaupungille uuden ohjelman. Loimaan kaupungin työntekijöiden palkka-aineistoon liittyen tuli 23.10.2020 esille tietoturvaloukkaus. Ohjelmistotoimittaja toimitti salattuna sähköpostina Loimaan kaupungin palkka-aineistoa vahingossa kolmannelle osapuolelle. Ohjelmistotoimittajan tietosuojavastaava valtuutettiin tekemään asiasta ilmoitus tietosuojavaltuutetun toimistoon. Lisäksi tietosuojavastaavalta pyydettiin listaukset henkilöistä, joita tietoturvaloukkaus koski ja mitä tietoja aineisto sisälsi.

Koska aineisto lähetettiin salattuna vain yhdelle henkilölle, jota koskee salassapitovelvoite, riskiä tietojen vuotamiseen ei ole. Näin ollen kyseessä on lievä tietoturvaloukkaus.

Kolmannen osapuolen tietosuojavastaavalta saatiin 28.10.2020 kirjallinen (sähköpostitse) ilmoitus, että aineistot hävitettiin asianmukaisesti.

Henkilöstöjohtaja tiedotti asiasta kaikkia kaupungin työntekijöitä 29.10.2020 henkilöstötiedotteella. Kyseisessä tiedotteessa kerrottiin tapahtumien kulku ja jatkotoimenpiteet. Saatuaan listauksen työntekijöistä, joita tietosuojarikkomus koski, tietosuojavastaava ilmoitti 2.11.2020 asianomaisille sähköpostitse ja kirjeitse (henkilöt, joilla ei ole sähköpostia) tapahtuneesta.

4. Kolmannen osapuolen palkka-aineisto saapunut sähköpostitse Loimaan kaupungin palkkasihteerille

Loimaan kaupungin henkilöstösihteeri ilmoitti 26.10.2020 saaneensa salattuna sähköpostina kolmannen osapuolen palkka-aineistoja.

Salattu sähköposti saapui kello 15:21 ja henkilöstösihteerin avattua viestin, hän huomasi aineiston sisältävän vieraita nimiä. Henkilöstösihteeri tarkisti, että löytyykö aineistoon merkittyjä henkilöitä palkkaohjelmasta.

Toisesta aineistosta selvisi henkilöiden olevan kolmannen osapuolen palkan-/palkkionsaajia. Loimaan kaupungin tietosuojavastaava sai tiedon kello 15:34. Sähköposti poistettiin kello 15:49.

Asiasta ilmoitettiin ohjelmistotoimittajalle. Lisäksi Loimaan kaupungin tietosuojavastaava keskusteli puhelimitse asiasta kolmannen osapuolen tietosuojavastaavan kanssa. Myöhemmin kolmannen osapuolen tietosuojavastaavalle ilmoitettiin kirjallisesti (sähköpostitse), että kaikki väärät tiedostot poistettiin.

Kyseessä oli lievä tietoturvaloukkaus.

5. Pääsy asiakasraportteihin

Osana järjestelmän muutoksia, ohjelmistotoimittajalla oli maanantaina 9.11 lyhytkestoinen virhetilanne käyttöoikeusprosessissa. Tämä mahdollisti hetkellisesti yhden asiakkaan yhdelle henkilöstösihteerille pääsyn Loimaan kaupungin asiakasraportteihin. Henkilöstösihteeri ilmoitti asiasta heti ohjelmistotoimittajalle ja käyttöoikeus poistettiin. Virhetilanne kesti muutamia tunteja.

Loimaan kaupungin tietosuojavastaava sai asiasta tiedon 16.11.2020 ohjelmistotoimittajan tietosuojavastaavalta.

EU:n yleisen tietosuoja-asetuksen artiklaan 33 viitaten ”Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä”, ilmoitusta tietosuojavaltuutetun toimistoon ei tehty johtuen seuraavista syistä:

- Tunnistettu henkilö, jolle väärä käyttöoikeus mennyt
- Henkilöllä salassapitovelvoite ja tietojen hyväksikäyttökielto
- Vastaanottaja ilmoittanut asiasta heti
- Käyttöoikeus poistettu nopeasti

6. Viranomaisen väärään osoitteeseen lähettämät asiakirjat

Kirjaamo on ottanut kahdesti vastaan toiselle viranomaiselle tarkoitetun ei-julkisen asiakirjan. Asiakirjat on toimitettu oikeaan osoitteeseen.

Lisäksi kirjaamoon on toimitettu yksi asiakirja, jossa oli väärä, ei-julkinen liite. Liite on poistettu.

Näistä ei aiheutunut riskiä asianomaisille.

LÄHTEET

Tietosuojavaltuutetun toimisto, 2020. https://tietosuoja.fi/tietoturvaloukkaukset

Yleinen tietosuoja-asetus, artikla 33, 2020. https://gdprinfo.eu/fi/fi-article-33