Liikenne- ja viestintäministeriö

Päiväys/Datum
27.9.2019
Dnro/Dnr
1448/04/2018
Viite/Referens
Toimenpidepyyntö LVM/2435/02/2018, väliraportti 30.9.2019

Liikenne- ja viestintäviraston 2. väliraportti liittyen liikenne- ja viestintäministeriön toimenpidepyyntöön

Sisältö

1 Toimenpidepyynnön ja väliraportin sisällöt 2

2 Suljettujen palveluiden keskeiset muutokset suhteessa edelliseen raporttiin 2

3 Kehityshankkeiden johtamiseen ja päätöksentekoon liittyvä arviointi 2

4 Toimenpiteet tietosuojan ja tietoturvan varmistamiseksi 3

4.1 Palveluiden tietoturvan tilanne 3

4.2 Palveluiden tietosuojan ja laillisuusarvioinnin tilanne 3

4.3 Palaute viraston tietoturvallisuuden sertifiointiauditoinnista 4

4.4 Kehittämisen toimintamallin käyttöönotto 5

5 Jatkotoimenpiteet palveluiden kehittämiseksi 5

5.1 Suljettuina olevat palvelut 5

5.2 Asiointialustan uudistaminen 5

5.3 Tietosuojan kehittäminen 6

5.4 Palveluiden ja järjestelmien tietoturvallisuuden arviointi 6

6 Viraston riskienhallinnan yhdenmukaistaminen ja kehittäminen 7

1 Toimenpidepyynnön ja väliraportin sisällöt

Liikenne- ja viestintäministeriö (LVM) on 19.12.2018 antamassaan toimenpidepyynnössä edellyttänyt Liikenne- ja viestintävirasto Traficomia kohdistamaan liikenteen keskeisiin palveluihin tietoturvallisuuden auditoinnin sekä raportoimaan, miten virastossa on kehitetty tietosuojaan liittyviä prosesseja ja miten virasto järjestää sisäisen tietoturvallisuuden ohjauksen. Auditoinnin tulee valmistua vuoden 2019 loppuun mennessä. Traficomin tulee toimittaa väliraportit 31.5.2019 ja 30.9.2019 mennessä. Loppuraportti tulee toimittaa 16.12.2019 mennessä.

Tässä väliraportissa kerrotaan keskeiset muutokset suhteessa edelliseen toukokuussa jätettyyn väliraporttiin, johtopäätökset keväällä 2019 suoritetusta johtamiseen ja päätöksentekoprosesseihin liittyvästä arvioinnista, toteutetuista tietoturvaa ja tietosuojaa parantavista toimenpiteistä, tietoturva-auditoinnin tilanteesta sekä keskeiset löydökset virastoon elokuussa 2019 kohdistuneesta ISO 27001 -tietoturvallisuusstandardin sertifiointiauditoinnista.

2 Suljettujen palveluiden keskeiset muutokset suhteessa edelliseen raporttiin

Traficom avasi 26.6.2019 asiakkaille suljettuna olleen Julkiset ajoneuvotiedot ja veronmaksu -sähköisen asiointipalvelun. Palveluun toteutettiin kevään 2019 aikana tietoturvan ja -suojan tarkistusten pohjalta edellytetyt toiminnalliset ja tekniset muutokset. Julkiset ajoneuvotiedot ja veronmaksu -palveluun tehtyjä muutoksia käytiin läpi edellisessä sähköisiä palveluja koskevassa väliraportissa, jonka Traficom antoi Liikenne- ja viestintäministeriölle 27.5.2019.

Keväällä 2019 toteutettiin Katakri 2015 vaatimuksiin pohjautuva tietoturva-auditointi myös OmaTrafin sähköisiin asiointipalveluihin liittyvään integraatioalustaan. Raportin tulokset saatiin 19.6.2019. Raportista ilmenneiden puutteiden korjaus-/muutostyöt palveluun ovat käynnissä, mutta palvelun toiminnan kannalta kriittiset puutteet korjattiin ennen Julkiset ajoneuvotiedot ja veronmaksu -palvelun avaamista. Muiden vielä suljettuina olevien palvelujen (Julkiset kuljettajatiedot, Julkiset vesikulkuneuvotiedot, Julkiset ilma-alustiedot ja Merenkulun pätevyyskirjan tarkistaminen) osalta on toteutettu kevään 2019 aikana tietosuojan vaikutustenarvioinnin mukaisia muutostöitä. Muutostyöt testataan ennen palveluiden käyttöönottoa.

3 Kehityshankkeiden johtamiseen ja päätöksentekoon liittyvä arviointi

Virasto teetti osana sisäisen tarkastuksen vuoden 2019 suunnitelmaa selvityksen sähköisten asiointipalveluiden kehittämisen prosesseista. Toimeksiannon suoritti viraston ulkopuolinen taho kevään ja kesän 2019 aikana. Tarkastuksen tavoitteena oli arvioida ja kartoittaa Traficomin sähköisten asiointipalveluiden kehityshankkeiden prosesseja sekä toimintatapoja johtamisen ja päätöksenteon näkökulmista. Tarkastuksessa huomioitiin myös sisäisen valvonnan ja riskienhallinnan näkökulmat sekä annettiin suosituksia kehityshankkeiden prosessien ja keskeisten toimintatapojen edelleen kehittämiseksi.

Tarkastus kohdentui toimintamalleihin, jotka olivat olleet käytössä entisessä Liikenteen turvallisuusvirasto Trafissa. Tarkastuksessa ei tehty kriittisiksi luokiteltavia havaintoja. Tärkeimpiä esiin tulleita kehityskohteita, kuten ohjeistuksen velvoittavuus

ja soveltuva projektinhallintakoulutus on jo huomioitu Traficomin uudessa johtamisen- ja kehittämisen toimintamallissa.

Muita tunnistettuja kehittämiskohteita olivat muun muassa toimintaympäristössä tapahtuvien muutosten huomioiminen kehitystehtävien yhteydessä. Riskienhallinnan osalta huomiota kiinnitettiin toimintamallin ja ohjeistuksen laajennukseen virastotasolle sekä kehitystehtävien riskiarviointien huomioimiseen osana viraston riskienhallintaa. Lisäksi havaittiin tarvetta tietosuojanäkökulman sisällyttämiseen kehitystehtäviin koko hankkeen ajaksi. Samalla kiinnitettiin huomiota tietoturvan ja tietosuojan koulutustasovaatimuksiin kehitystehtäviin osallistuvien henkilöiden osalta.

4 Toimenpiteet tietosuojan ja tietoturvan varmistamiseksi

4.1 Palveluiden tietoturvan tilanne

Traficom hankkii Liikenteen tietojärjestelmien käyttöpalvelut Valtorin hallinnoiman sopimuksen kautta. [Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Traficom on ottanut Katakri 2015 (perustaso STIV) -viitekehyksen palveluiden teknisen tietoturvan vähimmäisvaatimukseksi. Samalla virastossa on käyttöönotettu laajemmat ei-toiminnalliset vaatimukset, jotka tukevat edellytetyn suojaustason mukaisten digitaalisten palvelujen hankintaa, suunnittelua sekä toteutusvaiheita. Myös Liikenteen tietojärjestelmien digiturvallisuuden tasoa kehittävän hankeen sisältöä on arvioitu uudelleen, jotta toteutus noudattaa viraston johdon linjauksia.

[Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Tuotannossa olevien avattujen sähköisten asiointipalvelujen osalta Liikenneasioidenrekisterin julkisen liittymän eli Julkivallu -palvelun tietoturvaa on kehitetty yhdessä Ely-keskuksen kanssa. [Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

[Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Traficom toteuttaa tietoturvatestauksia ja auditointeja osana jatkuvaa sähköisten palvelujen ja tietojärjestelmien kehittämisen toimintamallia. Sovelluskehityksessä huomioidaan tietosuoja ja –turva yhteistyössä määritetyn substanssitoimialan, turvallisuuden ja tietohallinnon asiantuntijoiden kanssa vaikutusten- ja riskiarvioinnein sekä uhka-analyyseilla. Sovelluskehityksessä on laajennettu testausautomaation käyttöä ja tuotetun koodin laatua seurataan analyysityökaluin.

Traficomin tietohallintoon on perustettu kuukausittain kokoontuva tietoturvaryhmä, joka seuraa Liikenteen tietojärjestelmiin liittyvien tärkeimpien tietoturvaan kehityskohteiden etenemistä ja tietoturvan tilannekuvaa.

4.2 Palveluiden tietosuojan ja laillisuusarvioinnin tilanne

Suljettujen sähköisten palveluiden tietosuojaa ja henkilötietojen käsittelyn lainmukaisuutta on arvioitu Traficomin toteuttamilla vaikutustenarvioinneilla. Lisäksi ulkopuolinen arvioija on tarkastellut palveluiden laillisuusnäkökohtia huomioiden erityisesti yleisen tietosuojalainsäädännön vaikutukset. Tehtyjä arviointeja käsiteltiin jo Traficomin 27.5.2019 päivätyssä väliraportissa. Arviointien perusteella on todettu,

että tietojen luovutus käyttöönotettavista sähköisistä palveluista on liikenteen palveluista annetun lain mukaista.

Palveluiden kehittämisessä on kiinnitetty huomiota tietosuoja-asetuksen tietosuojaperiaatteisiin ja henkilötietojen väärinkäytön riskien pienentämiseen. Palveluiden tietosisältöä on minimoitu palveluiden käyttötarkoituksien mukaisesti. Palveluiden käytettävyys vain yksittäisluovutuksiin on toteutettu teknisillä rajoitustoimenpiteillä.

Suljettuna olleiden sähköisten palveluiden arviointi- ja kehitystyön seurauksena koko organisaatiossa on kehitetty osaamista ja kykyä arvioida ja havainnoida tietosuojan ja tietoturvan toteutumista käytännössä.

Traficom pitää tärkeänä, että sen palveluista saadaan palautetta, ja että tietosuojan ja tietoturvan toteutumista voidaan arvioida myös asiakkaan näkökulma huomioiden. Avatuista palveluista saatujen palautteiden perusteella ei ole viitteitä siitä, että avattujen sähköisten palveluiden laillisuutta pidettäisiin puutteellisena, tai että tietojen julkaiseminen palveluista katsottaisiin muuten epäasialliseksi. Traficom ei ole saanut tietosuojavaltuutetun toimistolta avattuja palveluja koskevia yhteydenottoja eikä Traficomin tietoon ole tullut sellaisia uusia seikkoja, joiden johdosta laillisuusnäkökohtia olisi arvioitu palveluiden avaamisen jälkeen toisin.

[Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto] Nykyhetkellä henkilöstö raportoi herkästi poikkeamaepäilyistä viraston turvallisuustoiminnolle, joka tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa toiminnan läpinäkyvyyden lisäämiseksi ja vastuuviranomaisen näkemysten huomioimiseksi toiminnassa.

4.3 Palaute viraston tietoturvallisuuden sertifiointiauditoinnista

Viraston johtamisjärjestelmän muodostavat toimintatavat ja menettelyt, joilla virasto varmistaa kykynsä saavuttaa sille asetetut tavoitteet. Johtamisjärjestelmän viitekehyksinä sovelletaan ISO-standardeja: laatu 9001, ympäristö 14001 ja tietoturva 27001. Virastoon kohdistui ulkoinen auditointi 19. - 23.8.2019. Kyseessä oli laatu- ja ympäristöstandardien näkökulmista laajennusauditointi ja tietoturvastandardin näkökulmasta uudelleensertifiointi- ja laajennusauditointi.

Auditoijat raportoivat viraston muutosjohtamisen olleen onnistunutta, sillä he tekivät toiminnasta runsaasti positiivisia havaintoja. Erityisesti turvallisuuskulttuurin ja turvallisuustietoisuuden systemaattisesta kehittämisestä sekä turvallisuuden hallintamallista tuli positiivista palautetta. Haastateltavat henkilöt kertoivat kokeneensa, että viraston johtamisessa painotetaan erityisesti tietoturva- ja suojan huomioimista jokapäiväisessä työssä. Auditoijat havainnoivat, että viraston johto on tietoinen jäännösriskeistä ja tilannekuvasta kokonaisturvallisuuden, riskienhallinnan ja häiriönhallinnan suhteen. Myös viraston riskienhallintamallissa havaittiin aiempaa kokonaisvaltaisempi ote. Lisäksi turvallisuuspoikkeamien aktiiviseen tunnistamiseen ja raportointiin on panostettu merkittävästi.

Auditoinnin tuloksena lieviä poikkeamia löytyi viisi (raportti julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto) ja lisäksi auditoijat kirjasivat erilaisia kehityskohteita. Poikkeamien korjaamiseksi on laadittu suunnitelma ja kehityskohteet on myös huomioitu jatkuvan parantamisen näkökulmasta. Poikkeamien korjaussuunnitelma käsiteltiin 9.9.2019 viraston johtoryhmässä ja poikkeamien korjaaminen on jo käynnissä. Johtamisjärjestelmä tullaan auditoimaan uudestaan huh-

tikuussa 2020, jolloin laatu- ja ympäristöjohtamista arvioidaan uudelleensertifiointi-auditoinnin näkökulmasta ja turvallisuuden hallintamalliin kohdistetaan seuranta-auditointi.

4.4 Kehittämisen toimintamallin käyttöönotto

Traficomin uusi kehittämisen toimintamalli otettiin käyttöön syyskuun alussa. Kehittämisen toimintamallia on rakennettu johdon antamien tavoitteiden mukaisesti. Yksi tavoitteista oli asianmukainen tietosuoja-, tietoturva- ja riskikäsittelyn varmistaminen kehittämisessä. Mallin yksi toimintaperiaatteista on kehittämisen läpinäkyvyys. Tämä mahdollistaa viraston kehitystehtävien priorisoinnin ja tarvittavien resurssien varmistamisen tärkeissä kehitystehtävissä. Toimintamallissa on pyritty siihen, että se skaalautuu eri kokoisiin kehitystehtäviin.

Jokaiselle kehitystehtävälle tunnistetaan mahdolliset riippuvuudet muihin kehittämistehtäviin ja jo olemassa oleviin palveluihin sekä tunnistetaan ja varmistetaan resurssit. Menettelyllä varmistetaan mm. kehitystehtävien tietosuojan ja -turvan vaatimuksenmukaisuus sekä kontrollien toteuttaminen kustannus- ja resurssitehokkaasti. Riskienhallinta on jatkuva prosessi kehittämisen elinkaarella.

5 Jatkotoimenpiteet palveluiden kehittämiseksi

5.1 Suljettuina olevat palvelut

Traficomin sähköisistä palveluista ovat vielä suljettuina julkiset kuljettajatiedot, julkiset ilma-alustiedot, julkiset vesikulkuneuvotiedot ja merenkulun pätevyystiedot. Palveluiden avaamista edellyttävät toimenpiteet ovat käynnissä. Kaikkien suljettuina olevien palveluiden (pl merenkulun pätevyystiedot) osalta käyttöönottosuunnitelma sekä laillisuus- ja vaikutustenarviointi on toteutettu. Merenkulun pätevyystietojen osalta laillisuus- ja vaikutustenarviointi sekä käyttöönottosuunnitelma ovat vielä osittain kesken. Seuraavaksi tullaan avaamaan julkiset kuljettajatiedot -palvelu.

5.2 Asiointialustan uudistaminen

Traficom on käynnistänyt keväällä 2019 kehityshankkeen, joka tulee uudistamaan nykyisen Liikenteen sähköisen asioinnin alustan arkkitehtuuriin ja kehittää palvelujen asiakaskokemusta mm. saavutettavuuden vaatimukset huomioivaksi. Uudistushanke tulee korvaamaan nykyisen OmaTrafin teknisen alustan.

Kehityshankkeessa toteutetaan ensivaiheessa määritetyt pilotit ajoneuvojen ja vesikulkuneuvojen omistajavaihdokseen liittyviin palveluihin. Lisäksi toteutetaan taustajärjestelmiin liittyvien projektien etenemisen mukaan uusia palveluja, kuten liikenneluparekisteriin ja Drone-rekisteriin liittyvät palvelut. Kehityshankkeessa uudistuu myös sähköisen asioinnin mobiilikäyttöliittymä. Hankkeen vaatimuksena on, että toteutus on Katakri 2015 perustason mukainen. Työmäärältään ja arvoltaan mittava kehityshanke jatkuu v. 2020 - 21.

5.3 Tietosuojan kehittäminen

Tietosuojan osalta on käynnistymässä syksyn aikana useita tietosuojan parantamiseen tähtääviä hankkeita. Traficomin johtoryhmä hyväksyi elokuussa viraston tietosuojaverkoston käyttöönoton. Verkoston toiminta käynnistyy lokakuussa 2019. Tietosuojaverkoston tavoitteena on jakaa tietoa, kasvattaa osaamista ja herättää keskustelua ajankohtaisista tietosuoja-asioista sekä helpottaa ja edesauttaa yhteisten hyvien käytänteiden luomista. Verkosto tuottaa tietoa turvallisuustoiminnolle Traficomin tietosuojan tilasta kokonaisturvallisuuden tilannekuvan muodostamiseksi. Verkosto kokoontuu kuukausittain ja sitä johtaa tietosuojavastaava.

Tietosuojaa kehitetään kuluvan syksyn aikana toteuttamalla tietosuojan sisäinen tarkastus. Tarkastuksen suorittaa viraston ulkopuolinen tarkastaja.

Henkilöstön tietosuojaosaamista tullaan kehittämään tarjoamalla yleistä tietosuojakoulutusta koko henkilöstölle ja kohdennettua koulutusta tietosuojaverkoston tietosuojalähettiläille. Koulutuksia tarjotaan sekä verkkokoulutuksina että seminaari- ja tietoiskutyyppisinä koulutuksina. Koulutukset käynnistyvät lokakuussa 2019.

Virastossa on tunnistettu tarve kartoittaa, mitä asiakkaat virastolta rekisterinpitäjänä odottavat, ja miten voimme palvella asiakkaitamme tietosuojan osalta paremmin. Käytännössä tämä tarkoittaa asiakkaiden tarpeiden tunnistamista, niiden aitoa ymmärtämistä ja näihin tarpeisiin vastaamista asiakkaan positiivisen palvelukokemuksen varmistamiseksi. Virastossa on tehty suunnitelmaa, kuinka asiakastutkimusta ja palvelumuotoiluprosessia sekä palvelumuotoilijaa hyödyntävä asiakaslähtöinen tietosuoja tullaan toteuttamaan. Tämä työ on vielä kesken, mutta työn valmistuttua viraston malli on hyödynnettävissä myös muualla julkishallinnossa.

[Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

5.4 Palveluiden ja järjestelmien tietoturvallisuuden arviointi

Viraston keskeisten palveluiden tietoturva-auditointeja tullaan jatkamaan edelleen vuoden 2020 puolella. [Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Keväällä ja kesällä 2019 arvioitiin kiireperusteisesti kansalaisten oma-asiointipalvelut ja suljettuina olevat palvelut, Ely-keskukselta siirtynyt Julkivallu-palvelu, rajapinnat muiden viranomaisten, sopimuskumppanien ja lukuun toimivien tahojen tietojärjestelmiin sekä tietojärjestelmän integrointiratkaisu.

Auditointihavainnot ovat antaneet aiheen arvioida Traficomin vastuulla olevien palvelujen ja palvelujärjestelmien tietoturvallisuutta laajemminkin. Viraston vastuulla on yhteensä yli 300 sähköistä asiointikanavaa, joten arviointia joudutaan kohdistamaan prioriteettijärjestyksessä.

Seuraavassa vaiheessa hyväksytyn arviointilaitoksen auditoinnit kohdennetaan mm. EU:n tasoisten, muiden maiden viranomaisten käyttämien palveluiden rajapintoihin. Tarkastelussa tulevat olemaan EUCARIS- ja Tachonet-palvelut.

Kansainvälisten rajapintojen tarkastelun jälkeen auditoinnit kohdistetaan mm. ilmailun ja meriliikenteeseen liittyviin järjestelmiin ja palveluihin. [Poistettu julkisuuslain 24§:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Ministeriön toimeksiantoon pohjautuvien arviointilaitoksen suorittamien auditointien lisäksi palveluiden ja tietojärjestelmien tietoturvaa arvioidaan normaaliin tapaan osana kehittämisen mallia.

6 Viraston riskienhallinnan yhdenmukaistaminen ja kehittäminen

Virastolle on laadittu johtoryhmän kesäkuussa 2019 hyväksyttyjen periaatteiden mukaisesti riskienhallintapolitiikka, joka on hyväksytty johtoryhmässä 23.9.2019. Riskienhallintapolitiikassa arviointikohteiden (projektit, resurssit ja hankkeet) omistajuus on nostettu johtoryhmän jäsenten tasolle, mikä nostaa johdon tietoisuutta riskeistä sekä mahdollistaa nopeatkin toimet resurssien suuntaamiseksi ongelmatilanteissa.

Riskienhallinnan tavoitteita ovat muun muassa hallita tapahtumista johtuvia riskejä siten, ettei organisaation toiminta ole uhattuna, mahdollistaa organisaation toiminnan jatkuvuus, turvata henkilöstön hyvinvointia, minimoida riskeistä aiheutuvia vahinkoja, mutta myös havaita potentiaalisia mahdollisuuksia, analysoida ja hyödyntää niitä.

Viraston keskeisiksi riskeiksi on määritelty muun muassa viraston toiminnan lyhyt- tai pitkäaikainen keskeytyminen, palvelutason heikentyminen, henkilövahinko, omaisuusvahinko, tiedon menetys tai muuntuminen, tietovuoto, lain rikkominen ja maineriski. Jatkossa myös jäännösriski tulee kirjallisesti hyväksyä arvioinnin kohteen omistajan toimesta.

Virastossa on otettu syyskuussa käyttöön sisäisen tarkastuksen ohjesääntö, jossa määritellyt toimintatavat ja toimenpiteet tulevat parantamaan pääjohtajan kokonaiskuvaa viraston toiminnasta.

Helsingissä 27.9.2019

Pääjohtaja Kirsi Karlamaa

Turvallisuusjohtaja Jari Ylitalo