ISACA Finland Chapter (Tietojärjestelmien tarkastus ja valvonta ry)

Lausunto

27.07.2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Nykytilakuvaus ("johdanto") luo hyvän pohjakuvauksen tarpeesta ja merkittävistä syistä itse työlle. Lukijan sekä asiantuntijiden näkökulmasta johdanto ei kuitenkaan selvästi tuo esille mitkä ovat ne konkreettiset syyt tai tavoitteet nykytilan muutokselle. Esimerkkinä tästä on mm. "Osa sääntelystä on uutta ja osa kymmeniä vuosia vanhaa" joka vaatisi selkeät esimerkit sekä vaikutukset mitä esimerkiksi kymmenen vuotta vanhat sääntelyt aiheuttavat. Asiantunitjoille vanhentunut lainsäädäntö sekä muuttunut maailma on selkeää, mutta yhtälössä on monta päättäjää joille nämä asiat eivät ole arkipäivää.

Johdannon loppupuolelle on lisäksi "...kiinteästi tietosuoja-asetuksessa tarkoitetun automatisoidun päätöksenteon...". Mikäli käsitellään vain tietosuojakokonaisuutta jää tavoitteellisesti lausunto tyngäksi. Tietoturvan kokonaisuuden huomioiminen yhdessä tietosuojan näkölulman kannalta olisi pitkäjänteisempää ja merkityksellisempää tavoitteiden kannalta, koska hyvää tietosuojaa ei saavuteta ilman pohjalla olevaa hyvää tietoturvaa. Näitä kahta ei tule sekoittaa toisiinsa, mutta eimyöskään arvioida erikseen, sillä muuten tietosuojan näkkulma jää juridiseksinäkäkulmaksi eikä täten vastaa tietosuojan ylläpidon haasteisiin jota tietotuvamekanismit tukevat.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Kohta on pääosin selkeä ja nostaa esille mm. koko tietojärjestelmä-termin ongelmallisuuden. Tietojärjestelmät tulkitaan turhan usein vain IT eli ns. ATK-laitteiksi, vaikka tänä päivänä tietojärjestelmistä puhuttaessa merkittävän tulevaisuuden vektorin luovat myös erilaiset (äly)laitteet sekä ns. IOT-laitteet. Kappaaleessa merkittävä kohta onkin sivulla 16 kohta "Tietojärjestelmiin kohdistuvaa sääntelyä voidaan lähestyä ainakin seuraavista näkökulmista", joka tuo merkityksen esille eli kattavuuden lähes kaikkeen mitä yritykset ja hallinnonalat tänä päivänä tekevät.

Täydennystä ja konkretisointia vaatisi se, että lähes kaikki laitteet (jotka on verkotettuna oli kyseessä sitten tuottavateollisuus taikka terveydenhuolto) tulisi olla tietojärjestelmien sääntelyn alaisuudesta toimialasta taikka laitteen käyttötarkoituksesta riippumatta.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Tämän päivän tietojärjestelmien monimuotoisuus, sisältöpitoisuus ja muuttavat käyttötarkoitukset lisäävät ennakkovastuita ja vaatimuksia niin omistajalle/tilaajalle kuin myös palvelun toimittajalle/ylläpitäjälle/kehittäjälle. Nämä mahdollisuudet ja vastuut tulisi vahemmin koskea myös tietosuoja ja tietoturvavaatimuksia.

Toiminnallisesta näkökulmasta tietojärjestelmille tulisi pystyä vaatimaan paremmat lähtökohdat tulevaisuuden muutoksille ja kehityksille. Toiminnallisesti yhteiskunnallinen yhteentoimivuus, luotettavasti tiedon siirtäminen (myös turvaluokitellun tiedon) kuin myös ylläpidollisen sitoutumattomuuden pitäisi olla johdetumpaa. vaatimustenmukaisuudella pystytään saavuttamaan jo tiettyjä kokonaisuuksia, mutta käytännöntasolla toiminnassa on vielä merkittäviä heikkouksia. Toiminnallisia vaatimuksia käsitellään liiankin toimintolähtöisesti, ei strategisesti tai mukautuvasti. Tämä näkyy erityisesti kun puhutaan yhteiskunnallisesti kriittisten järjestelmien yhteentoimivuuden näkökulmasta (joka peilautuu myös heikkona tietoturvana ja vaihtelevina käytäntöinä).

4. Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

Järjestelmien tulisi kasvavassa määrässä hyödyntää esimerkiksi pilvipalveluiden mahdollisuuksia niin lainsäädännön kautta kuin myös prosessien toiminnan näkökulmasta. Koska muutokset toimintaympäristöissä tapahtumat aikaisempaakin tietojärjestlemä lähtöisesti, on huomioitava että mikä tänään on uutta, on kohta jo vanhentuvaa. Huomioitavaa on kuitenkin, että kansallisesti kriittisten järjeltelmien kehitys "kotikutoisesti" ei ole kustannustehokasta ja pyörää ei kannata keksiä uusiksi. Merkittävää onkin varhaisen vaiheen riskienhallinnalliset menetelmät ja balansointi sekä mekanismien rakentaminen jolla a) palveluissa voidaan turvallisesti käsitellä turvallisuuskriittistä informaatiota ja b) vastuut on muutenkin kuin paperilla määritelty.

Ns. toimitusketjujen (lue: IT-kumppanit / vast.) vastuita tulisi kasvattaa kokonaisuudessa ja heiltä tulisi kriittisten järjestelmien osalta vaati laadukkaampaa tietoturvaa/-suojaa. Tekniset vaatimukset koskevat valitettavan usein minimitasoa ja tietoturva/-suoja on kohta jossa leikataan liikaakin tai oletetaan sen olevan hyvällä tasolla. Auditointi ei ole ratkaisu vaan vain yksi mekanismeista. Sen sijaan tietoturva tulisi rakentua aina alkuideoinnista lähtien rampauttamatta toiminnallisia tavoitteita.

5. Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

Dokumentaation osalta Suomessa on vielä liiaksi vaatimuksena vain Suomeksi dokumentointi. Tällöin terminologia saattaa poiketa alan standardeista tai dokumentaatiossa uusille teknologioille "keksitään" soveltuvia termejä. Tämän kaltaiset käytännöt saattavat heikentää ylläpidettävyyttä, kestävyyttä ja ongelmaratkaisua pitkän päälle, erityisesti jos kumppanit vaihtuvat matkan varrella.

Näiden epäselvyyksien kustannusvaikutukset saattavat tuntua pieniltä mutta näkyvät kasaantuvana merkittävästi. Siksi suotavaa olisikin vaati myös englanniksi olevaa dokumentaatiota (tai jopa vain englanniksi olevaa dokumentaatiota), joka mahdollistaisi laajemmat mahdollisuudet käyttää kansainvälisiä resursseja vastaamaan jo näkyvään resurssiongelmaan mikä alaa koskee.

Toinen merkittävä asia on dokumentaation laatu ja ylläpito mitä tulee kumppaneille asettaviin vaatimuksiin. Kun sopimusteknisesti vaaditana dokumentaatiota tehdään se turhan usein "sinnepäin" tai siihen ei ole resursoitu/budjetoitu riittävästi jotta taso olisi hyvä. tätä dokumentaatiota tulisi tilaajien myös vaatia aiempaa näkyvämmin ja osallistuvammin.

Kehittämisen osalta tulisi vaatia myös aiempaa parempi tietoturvatoimia. Nykyiset auditoinnit ovat pintaraapaisu, ja ns. SDLC/DevSecOps eli kehityksen aikana tapahtuva tietoturvavarmistus on matalalla tasolla. Toimittajilta vaaditaan tietoturvatoimia, mutta näiden valvonta on vielä todella vaihtelevalla tasolla. Syitä on mm. resurssipula, osaamattomuus ja epätieto/luotto kumppanin toimiin.

6. Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

Virkavastuuta pystyvät virkamiehet kommentoimaan paremmin, mutta turvallisen kehittämisen onnistumisen kannalta vastuuta tulisi olla niin tilaajalla kuin myös kumppanilla joka toteuttaa. Mikäli jompikumpi tahoista karsii kustannussäästösyistä tietoturva/-suoja asioista pitäisi sanktiot/vaikutukset olla nykyistä merkittävämmät.

7. Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

Kuten aiemmissa kohdissa jo kommentoitu, laatu ja käytettävyys lähtee jo alkuvaiheen huomioimisesta ja suunnitelmista. Käyttöä tulisi harkita laajemmassa kuin vain oman organisaation kontekstissa, sillä yhteiskunnallinen yhteentoimivuus ja luotettavuus on digitalisoituvassa yhteiskunnassa menestystekijä. Mikäli päätöksiä halutaan automatisoida täysin, on luottamus laatuun oltava merkittävä. Se asetta reunaehtoja niin teknisesti kuin myös hallinollisesti. Tietovarantojen vaikeus on niiden monimuotoisuus, jotta automatisointia tai yhteiskäyttöä voisi harkita. Lainsäädännöllisesti tämä voisi tarkoittaa yhtenäistä linjausta tietoaineiston muodosto, tasosta jne. jolla voi olla merkittäviä kustannusvaikutuksia varsinkin ns. legacy-järjestelmät huomioiden.

Tämä kohta saattaa muodostua erittäin haastavaksi vaikka ja siirtymäaika voi olla merkittävä.

8. Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

Aiemmissa kohdissa tätä jo kommentoitu laajasti, mutta ns. audit-lähtöinen varmistus ei vastaa enää tämän päivän haasteisiin. Tarkastuksia tullaan tarvitsemaan jatkossakin, mutta ns. kontrollien kautta tehtävä arviointi jää liiankin pintaraapaisuksia. Siksipä tietoturvaa tulisi arvioida ja testata jatkuvasti

niin järjestelmänäkökulmasta kuin myös organisaation hallinnollisesta näkökulmasta (=miten johdetaan ja valvotaan, mitataan ja kehitetään).

Lisähuomiona tulisi tunnistaa myös toimitusketjujen vastuu. Nykyisellään tarkastukset ovat suhteellisen vähäisiä tai läpinkymättömiä järjestelmän omistajan suuntaan mitä tulee kumppaneiden vastuisiin. Tekemättä jääneet tietoturvatehtävät tulevat esille vasta ongelmien noustessa esiin, kumppania vaihdettaessa tai hyökkäysten/tietomurtojen yhteydessä. Yhteiskunnallisesti luotetaan liiaksi tilanneraportteihin ja oletuksiin, mutta kunnollisia testauksia tulisi toteuttaa ja vaati niiden myötä enemmän kumppaneilta. Kumppaneilta tulisi vaati jatkuvaa kehityksen aikana tapahtuvaa tietoturvatyötä ja monitorointia muutenkin kuin paperilla. Eri yhteisöissä tästä on keskusteltu ja esille on nostettu mm. minimibudjettiosa mikä tulisi asettaa tietoturvalle kehitystyössä, joka ei ole sulautetettu osaksi muuta kustannusta vaan sen pitäisi kohdistua suoraan tietoturva-/tietosuojatyölle osana tietojärjestelmä kehitystä (ja kumppaneilta vaaditaan läpinäkyvyys tähän).

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Muistiossa on hyvää pohdintaa ja valmistelua on selvästi tehty muutenkin kuin lainsäädännön näkökulmasta. Muutamassa kohdassa nostettu toimitusketjujen (mm. IT-toimittajat) vastuu tulisi kuitenkin huomioida osana kokonaisuutta niin vastuiden kuin myös käytännön velvollisuuksien näkökulmasta. Ilman heidän panosta, osallistumista ja sitouttamista voi lainsäädäntö jäädä paperilla kauniiksi,mutta käytännössä vaihtelevaksi/tulkinnanvaraiseksi.

Toinen huomio on myös soveltuvuus eri toimialojen/hallinnonalojen kuten myös kokoluokkien organisaatioille. Mikäli lainsäädäntöä ei saada riittävän selväksi ja yksiselitteiseksi näen tässä kaksi mahdollista kompastuskiveä: 1) Virkamiehen vastuu asioihin joissa asiantuntemusta ei ole omassa hallinnonalassa/toiminnassa ja 2) Merkittävät vaikutukset IT-palveluiden kokonaiskustannuksiin joka syö resursseja kehityksestä/vaatii kompromisseja jättäen tavoitteiden saavuttamisen kauaksi oletuksista.

10. Muut yleiset kommentit arviomuistiosta

-

Marjomaa Niko
ISACA Finland Chapter (Tietojärjestelmien tarkastus ja valvonta ry) - ISACA hallitusen jäsen ja tietoturva-asiantuntija