Liikenteenohjausyhtiö Fintraffic Oy

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

1. Tietoturvaa tulisi lähtökohtaisesti tarkastella erilaisissa toimintaympäristöissä/skenaarioissa tapahtuvana toimintana:

1. Normaali tuotannollistaloudellinen ympäristö, jossa rikolliset/valtiolliset toimijat vaikuttavat satunnaisesti

2. Ympäristö, jossa rikolliset/valtiolliset toimijat vaikuttavat aktiivisesti

3. Joku toimija aktiivisesti yrittää vaikuttaa/rikkoa tietyn ympäristön (esim. hybridisodankäynti/sotaa edeltävä tila)

4. Sotaa muistuttava tila, jossa huoltovarmuustoimenpiteitä tarvitaan aktiivisesti

Tietosuojaympäristöt olisi syytä luokitella erikseen ja tarvittavat toimenpiteet määritellä erilaisten skenaarioiden näkökulmasta. Tietosuojan merkitys suurin skenaarioissa 1. ja 2. Esim. jos vuotanut tieto saattaa johtaa identiteettivarkauteen, tällaiset skenaariot on myös huomioitava tietoturvan varmistamisessa

Ehdotuksena on jatkaa tieto- ja kyberturvallisuuden sekä tietosuojan kehittämistä yhteiskunnan kriittisillä toimialoilla erillisissä työryhmissä esimerkiksi Kyberturvallisuuskeskuksen johdolla.

2. Tietoturvaan liittyvät roolit sekä vastuut, velvoitteet ja oikeudet olisi selkeytettävä. Lainsäädännöstä tulisi yksiselitteisesti ilmetä, mikä viranomainen/taho (tiedonhallintayksikkö), vastaa valtakunnallisten tietojärjestelmien ja tietovarantojen tiedonhallinnasta, niiden suunnittelusta ja toiminnasta sekä tietosuojan ja tietoturvan toteuttamisesta. Myös julkista

hallintotehtävää hoitavien tahojen ja/tai valtion erityistehtävää hoitavien yhtiöiden asema tiedonhallinnan, tietojen luovutusten sekä tietosuojan ja tietoturvan osalta tulisi määrittää yksiselitteisesti. Näkemyksemme mukaan tietosuoja-asetuksen mukaista rekisterinpitäjyyttä ja tiedonhallintalain mukaista tiedonhallintayksikön ja tietoturvavaatimuksista vastaavan tahon roolia ei olisi syytä eriyttää toisistaan. Erityisesti silloin, kun tiedonhallintaan liittyvä julkinen hallintotehtävä on laissa säädetty sopimuksella annettavaksi tai ulkoistettavaksi yksityiselle toimijalle, niin lakisääteinen ja käytännön tosiasiallinen vastuu esimerkiksi liikenteestä kerättävän tiedon tiedonhallinnasta, tietosuojasta- ja tietoturvasta jää epäselväksi. Hallinnon laillisuusperiaatteen mukaisesti viranomaisen tai julkista hallintotehtävää hoitavan toimijan tehtävien - ja myös tiedonhallinnan - tulisi perustua lainsäädäntöön.

Yhteisrekisterinpitäjyyteen sekä usean eri viranomaisen hyödyntämien tietojärjestelmien ylläpitoon ja käyttöön liittyvää roolitusta ja vastuita tulisi selkeyttää lain tasolla.

Lisäksi tulisi selventää, kuuluvatko julkista hallintotehtävää hoitavat tahot / valtion osakeyhtiöt Kyberturvallisuuskeskuksen neuvontapalveluiden ja koulutuksen piiriin.

3. Kuten raportissa on todettu, niin liikenteen toimialalla tietoturva- ja tietosuojavaatimuksista ei ole säädetty suoraan laissa, vaan vaatimuksissa on hajontaa eri viranomaisten kesken sekä erilaisia tulkintoja toimialan sisällä. Liikenteen toimialaa koskevat yhdenmukaiset tietoturva- ja tietosuojavaatimukset tukisivat liikenteen ohjaus- ja hallintapalvelun yhteydessä kerättävän tiedon ja muun liikennetiedon hallinnan keskittämistä sekä liikennetiedon ekosysteemin toteuttamista. Huomiota olisi kiinnitettävä erityisesti huoltovarmuuden kannalta tärkeiden tietojärjestelmien, tietoliikenneteknisten prosessien ja toimintojen tietoturvaan, vaikka tietojärjestelmän sisältämät tiedot sinänsä eivät olisi julkisuuslain nojalla salassa pidettäviä tai turvaluokiteltuja. Tämän vuoksi ISO27001 -sertifiointiehdotus kuulostaa erittäin järkevältä.

4. On huomioitavaa, että tieto -ja kyberturvallisuuden haaste ei ole puhtaasti lainsäädännöllinen tai hallinnollinen, vaan taloudellis-tuotannollinen ongelma, josta näkökulmasta tätä olisi hyvä lähteä purkamaan. Myös viranomaisten ja yritysten riskinhallintaan ja tietoturvaan liittyvän osaamisen kasvattamiseen ja ymmärryksen lisäämiseen tulisi kiinnittää huomiota. Riskienhallinnan perusteella on tärkeää varmistaa investoinnit tietoturvan ja kyberturvallisuuden kannalta relevantteihin alueisiin. Esim. vaade tiedon säilyttämisestä suomalaisessa konesalissa ei takaa riittävää tietoturvaa, jos tietoturvan taso, havainnointi- ja reagointikyvykkyys sekä sietokykyisyys ei ole paikallaan. Tämä lisää vaan kustannuksia väärään paikkaan, eikä investoinnit kohdistu sinne, missä niitä kipeästi tarvitaan.

5. Julkisissa kilpailutuksissa on prosessimielessä hankalaa kilpailuttaa tietoturvaa ennakoivasti, pitkäjänteisesti ja kattavasti, tämän lisäksi tietoturvatarpeiden muuttuessa ajaudutaan helposti uuteen kilpailutukseen. Myös Hanselin resursseja ja osaamista tulisi vahvistaa, mikäli Hanselin halutaan ottavan suurempaa roolia merkittävissä tietoturvaan ja kyberturvallisuuteen liittyvissä

hankinnoissa. Hanselin ja/tai JHNY:n kautta olisi tarkoituksenmukaista järjestää keskitetysti tietoturvaan liittyvän yleisen osaamisen vahvistamista kaikille hankintayksiköille.

6. Julkisen sektorin hankinnoissa yleisesti käytössä olevat Hanselin tietoturvasopimukset pitäisi päivittää mahdollisimman pikaisesti ajan tasalle, tämän hetken vaateet aiheuttavat lisäkustannuksia ja tietoturvavaatimukset kohdistuvat vääriin alueisiin ja konkretia puuttuu.

7. Valtorilla ei ole riittävän hyvin läpinäkyvästi mittaroituja palveluita käytössä, jotta heillä olisi luotettavasti riittävän laadukkaat palvelut ja että tietoturvan tilaa voisi seurata systemaattisesti.

8. Ei ole 100% tietoturvaa, joten havainnointi- ja reagointikyvykkyyttä on syytä korostaa joka alueella.

9. Rikolliset toimivat järjestelmällisemmin ja yhteistyössä tiiviinä ryhmänä, joten julkisen sektorin pitäisi pystyä yhtä tiiviiseen yhteistyöhön ja riittävään tieto- ja kyberturvallisuuden osaamisresursointiin jokaisen toimijan osalta. Siiloutumista pitäisi estää monella eri tasolla, toimivaltarajat estävät osittain tällaisen yhteistyön.

10. Suomalainen tietovarantojen suojaamisen taso vaihtelee, jonka vuoksi tarvitaan ajantasaista ja järjestelmällistä auditointia/raportointia. Tilannekuva on puutteellinen ja sitä olisi syytä kehittää kansainvälisen vaatimustason ja maailmalla havaittujen uhkien mukaisesti (ei pelkästään kansallisen), koska se vaikuttaa suomalaisen yhteiskunnan kilpailukykyyn. Esim. Kybermittari tähtää vertaisarviointiin Suomen sisällä, vaikka meidän kannattaisi verrata itseämme kansainvälisesti esim. ISO27001 & ISO27002, sekä ISF parhaat käytännöt.

11. Auditoinneissa olisi dokumenttien katselmoinnin sijasta syytä keskittyä teknisiin tietoturva auditointeihin, jossa auditoidaan sitä, mikä oikeasti on tietoturvan taso, havainnointi- ja reagointikyvykkyys sekä sietokykyisyys.

12. Mobiilipäätelaitteeseen asennettava sovellus ei välttämättä ole se paras vaihtoehto, jos on tarkoitus välittää salaiseksi luokiteltavaa tietoa esim. hyökkäysyrityksistä. Tärkeintä olisi siis ymmärtää ensin, keneltä on tarkoitus kerätä tietoa, mitä tietoa ja kuka sitä hyödyntää ja mihin. On syytä ymmärtää myös, kenelle analysoitua tietoa voidaan jakaa ja millä tasolla tietoturvan on oltava, onko sovelluksen ja mobiilipäätelaitteen yhdistelmä riittävän turvallinen tätä varten - jokaisessa mobiilikäyttöjärjestelmässä. Jos on tarve kerätä kansalaisilta tietoa ja jakaa heille tietoa keskitetyn sovelluksen kautta, voisiko sitä varten hyödyntää jo olemassa olevaa sovellusta esim. 112 sovellusta.

Viranomaiselta saatavilla oleva kyberturvallisuustieto on hajautettu eri palveluihin ja kommunikointikanavat viranomaisen ja yhteistyötahojen kanssa ovat vaihtelevia.

Kyberturvallisuuskeskuksella käytössä olevat kommunikointikanavat sisältävät muun muassa verkkosivut, uutiskirjeet, tietoturvaloukkaus -lomakkeet, erilaisia julkisia ja toimialakohtaisia postituslistoja, sekä muita julkisia- ja vain tietyille toimijoille tarkoitettuja kommunikointipalveluita.

Kehitettävä palvelu voisi yhdistää Kybertuvallisuuskeskuksen tilannekuvapalvelut sekä kommunikointikanavat ja mahdolliset muut viranomaistiedot yhteen portaaliin, joka mahdollistaisi esimerkiksi yritysten tietoturvasta vastaaville tahoille keskitetyn näkymän viranomaispalveluihin kyberturvallisuusasioissa. Palvelu voisi sisältää asianhallintajärjestelmän tietoturva-asioiden, kuten tietoturvaloukkausten käsittelyn seurantaan, turvalliseen viestintään sekä erilaisten tilannekuvapalveluiden uutisvirran.

13. Toiminnassa ei pitäisi pelkästään keskittyä lainsäädännönmukaisuuteen, vaan fokuksen olisi oltava myös tuloksissa niin, että oikeasti tietoturvaa ylläpidetään sekä ollaan sietokykyisiä ja vastustuskykyisiä kyberhyökkäysten sattuessa. Rikolliset toimivat lainsäätäjää ketterämmin. Jos yritämme ratkaista näitä asioita pelkästään lainsäädännön ja hallintamenetelmien kautta – olemme aina jäljessä.

14. Tarvitsemme Suomessa tieto- ja kyberturvallisuuden kulttuurimuutosta ja osaamisen vahvistamista. Fokus ei saisi olla pelkästään lainsäädännössä ja dokumenteissa, vaan myös toiminnan jalkauttamisessa, esim. aluevastuuperiaate ei välttämättä toimi osaamisen puutteen vuoksi. Uusi digitalisaation ja kyberrikollisuuden maailma tulisi ottaa huomioon esim. poliisiammattikorkeakoulun tutkintorakenteessa, täydentävissä koulutuksissa tai rekrytoinneissa. Teknistä tietoturvaosaamista ei välttämättä saavuteta pelkällä koulutuksella – osaamista kun tarvitaan laajasti esim. verkko, tietokannat, pilvipalvelut ja työasemat ymmärtämisessä. Olisiko järkevää hakea IT ammattilaisten ryhmästä henkilöitä, joille tietoturvaa koulutettaisiin – koulutusaika lyhenisi huomattavasti.

Miten kulttuurimuutos ja osaamisen vahvistaminen varmistetaan viranomaispuolella avainhenkilöiden sekä jokaisen työntekijän osalta roolinsa mukaisesti? Avainhenkilöitä olisi syytä kouluttaa säännöllisesti ja varmistua osaamisen tasosta.

15. Onko kyberturvallisuusstrategiassa ja sen toimeenpano-ohjelmassa huomioitu riittävä rahoitus? Nykyisillä investoinneilla emme ole päässeet pitkälle. Tähtäämmekö edelleen siihen, että olemme kyberturvallisuuden ykkösmaita ja onko määritelty mitä ykkösmaana olo käytännössä tarkoittaa, mitä teemme, mitä emme tee.

16. Pienten yritysten osalta sertifiointi ei ole itseisarvo, vaan malli, mitä pieneltä yritykseltä ostetaan. Jos pienellä yrityksellä on hyvä tuote, riskejä voi pienentää auditoimalla itse tuote ja varmistamalla tuotteen ylläpito järjestelmässä, jonka toimittaa joku kyvykkäämpi yritys, jolla riittävät resurssit tietoturvan ylläpitoon.

17. Suomalaisen yhteiskunnan täytyy valmistautua kvanttiteknologian tuloon ja sen kyberturvallisuus vaikutuksiin. Muutokset täytyy aloittaa nyt, jotta Suomelle kriittiset toimialat säilyttävät kilpailukykynsä.

Väliraportin muut osat, kommentit:

-

Korvenoja Riikka
Liikenteenohjausyhtiö Fintraffic Oy