Puolustusvoimat

Lausunto

05.10.2016

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohjeen rakenne on selkeä. Ohje etenee loogisesti käsittelykyvyn muodostamisesta aina poikkeamatapahtumista toipumiseen. Teksti on selkeää, johdonmukaista ja ymmärrettävää. Taulukoita ja kuvia on käytetty hyvin havainnollistamaan tekstiä. Asiaan liittyvä lainsäädäntö on hyvin esillä ja koottuna myös erilliseksi liitteeksi. Esimerkkejä ja tekstiä selventäviä asioita on koottu liitteiksi sopivasti.

1. Johdanto

Lausuntomme:

On riittävä.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Poikkeamien käsittelyn vaiheet on kuvattu selkeästi ja huomioitu hyvin myös mahdollinen paluu prosessissa aiempiin vaiheisiin.

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

”Ohjeluonnoksen luvussa 3 Tietoturvapoikkeamien käsittelykyvyn muodostaminen käytetään käsitteitä organisaatio, virasto ja viranomainen ongelmallisesti tai jopa virheellisellä tavalla. Viranomaisten toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki) 4 §:ssä säädetään viranomaisesta ja tässä tarkoituksessa mm. viranomaisen velvollisuudesta suunnitella ja toteuttaa asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyn niin, että tietojen suoja, eheys ja laatu turvataan asianmukaisin tietoturvallisuusjärjestelyin ja huomioon ottaen tietojen merkitys ja käyttötarkoitus, tietoon kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset (JulkL 18 § 1 mom. k 4). Julkisuuslain 36 §:n

nojalla annetuissa asetuksissa, asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999) sekä valtioneuvoston asetus tieto-turvallisuudesta valtionhallinnossa (681/2010), tarkennetaan edelleen tästä johtuvia viranomaisen velvollisuuksia. Julkisuus- ja salassapitolainsäädäntöä koskevan täytäntöönpanon yhteydessä on siten aina kysymys viranomaiselle kuuluvan toimivallan; velvollisuuksien ja oikeuksien tarkastelusta.

Useista viranomaisista muodostuvien valtion virastojen tai laitosten yhteydessä, esim. puolustusvoimat, on arvioitava viranomaisten erillisyyden merkitystä asiakirjojen julkisuutta ja salassapitoa koskevan päätöksenteon yhteydessä. Näin siksi, että oikeuskirjallisuudessakin esitetyn mukaisesti jokainen viranomainen, hallintoyksikkö arvioi ja harkitsee itsenäisesti julkisuuslain 14 § nojalla, onko sen hallussa oleva asiakirja julkinen. Tätä lain soveltamiseen liittyvää harkintavaltaa ei voida ohjata tai rajoittaa hallinnon sisäisin määräyksin tai ohjein. Viranomaisen itsenäisyyden kääntöpuoli on viranomaisen velvollisuus käyttää päätösvaltaansa lain mukaisesti. Näin ollen julkisuutta ja salassapitoa koskevien ratkaisujen, ja tästä johtuen myös tietoturvallisuusjärjestelyjen ja -menettelyjenkin yhteydessä, on huomioitava ensisijaisesti viranomainen ja viranomaisten erillisyyden merkitys.

Se, että hallinto on järjestetty alaisuus- ja valvontasuhteisiin, ei merkitse poikkeusta tästä viranomaisten erillisyydestä. Viranomaisten erillisyys edellyttää kuitenkin aina harkintaa sen suhteen missä asiassa hallintoyksikkö on toimivaltainen ja missä määrin toimivalta kuuluu Pääesikunnalle tai muulle ylemmälle esikunnalle. Samaan virastoon kuuluvien viranomaisten keskinäinen suhde perustuu keskushallintotason viranomaiseen tehtäviin ohjata voimassa olevasta laista johtuvaa toimeenpanoa siten, että se tapahtuu mahdollisimman tehokkaasti ja kustannukset huomioiden (ns. hallinnon tehokkuusvaatimus). Tämä tapahtuu erilaisin hallinnollisin määräyksin ja ohjein.

Näyttää siltä, että VAHTI-ohjeissa toimeenpanon ohjaus on vakiintunut myös organisaatioon kohdistuvaksi. Tämä ilmentää selvästi mm. Olli Mäenpään esittämää kehitystä siitä, että julkisessa hallinnossa on alettu enenevässä määrin soveltaa yksityiseltä sektorilta, yritystoiminnasta ja standardeista, lainattuja malleja ja ilmaisuja. On kuitenkin selvää, että viranomaistoiminnassa tulisi jo oikeusvarmuudestakin johtuen pitäytyä tarkemmin niissä käsitteissä, jotka lainsäätäjä on tähän tarkoitukseen määritellyt. Viranomaisen käsitteen lisäksi tämä pätee yhtä lailla VAHTI-ohjeistuksen myötävaikutuksella tapahtuneeseen ”tiedon omistaja” määrittelyn vakiintumiseen; tällaiselle ei ole löydettävissä perusteita lainsäädännöstä. On selvää, että esim. julkisuuslain 13- 16 §:issä tarkoitetuissa tiedon antamista koskevissa tilanteissa on kysymys toimivaltaisen viranomaisen tunnistamisesta; eikä tämä sääntely edes mahdollista minkäänlaista ”tiedon omistamisen” näkökulmaa. Mikäli VAHTI-ohjeistuksessa aiotaan edelleenkin pitäytyä käsitteessä organisaatio, on se varmin tae sille, että viranomaisten keskinäiset toimivaltasuhteet ja niihin perustuvat vastuut jäävät epäselviksi.”

Taulukossa 1 olisi hyvä huomioida, että viraston johto päätöksenteosta vastaavana ei välttämättä ole todenmukainen maininta. Isommissa organisaatioissa kaiken tietoturvapoikkeamiin liittyvän päätöksenteon vieminen viraston johdolle ei ole mahdollista eikä myöskään järkevää. Sen vuoksi esitetään tässä käytettävän muuta termiä, esimerkiksi vastaava viranomainen.

Lisäksi taulukossa 1 voisi käyttää palvelun omistajan asemesta julkishallintoon sopivaa termiä toimivaltainen viranomainen.

Taulukossa 3 on kuvattu niitä tapauksia, joissa on ilmoitusvelvollisuus. Peruste-sarakkeessa on annettu lait, asetukset ja määräykset, joihin ilmoitusvelvollisuus perustuu. Näiden kunkin osalta tulisi kuvata ko. lain, asetuksen tai määräyksen nimi ja tunnus. Nyt näitä on kuvattu epäyhtenäisesti.

VIRT-toiminta tulisi kuvata hieman tarkemmin. Mukaan tulisi sisällyttää, mikä on VIRT-toiminnan peruste (laki, asetus, määräys, muu?) ja mitä toimijoita VIRT-toiminnassa on mukana.

Luvussa 3.4 pitäisi tuoda esille lokien osalta selkeämmin henkilörekisteriseloste-vaatimus ja milloin se tulee tehdä. Lisäksi viitattaessa tekstissä lakiin ensimmäisen kerran, tulisi lain nimen yhteydessä mainita lain tunnus (esim. Tietoyhteiskuntakaari (917/2014)). Lokien osalta olisi myös hyvä mainita erilaisiin lakiperusteisiin perustuvat lokien säilytysaikavaatimukset, jotta lokien suunnittelun yhteydessä voidaan varautua tilanteen mukaan oikean mittaisiin säilytysaikoihin ja liittyviin tallennuskapasiteetteihin. Säilytysaikavaatimukset voisivat olla esimerkiksi erillisenä liitteenä.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Ei muutosehdotuksia tähän lukuun.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Todistusaineiston turvaamisen osalta on syytä myös kiinnittää huomiota siihen, että etukäteen selvitetään, kenellä on oikeus suorittaa esim. tietokoneen takavarikointi, jotta tilanteen ollessa päällä toimitaan kaikilta osin lainsäädännön mukaan.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Luvussa on huomioitu hyvin poikkeamista oppimisen tärkeys. Vielä voisi ehkä lisätä, mitkä organisaation osat on otettava mukaan jälkianalyysiin.

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

-

Liitteet 2-5

Lausuntomme:

-

Liitteet 6-9

Lausuntomme:

-

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Vaatimukset on hyvä kuvata, mutta kysymys herää, miten tämä vaatimustaulukko on linjassa meneillään olevan ”100-vaatimusta” hankkeen kanssa, jossa tavoitteena määritellä eri osa-alueitten osalta vain minimivaatimukset. Eli miksi ohjeistus perustuu näiltä osin nyt edelleen perustason, korotetun ja korkean tason vaatimuksiin, jos samanaikaisesti toisen VAHTI-työryhmän tavoitteena on ohjeistuksen perustaminen ”minimivaatimuksiin”?

Muuten vaatimuksista sinänsä ei ole kommentoitavaa, kattava ja keskeiset kokonaisuudet mukana.

Ehdotetut perustason vaatimukset ovat

-

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIlle?

-

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Hyvin

Koljonen Pasi
Puolustusvoimat