Oikeusrekisterikeskus

Lausunto

10.10.2016

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Oikeusrekisterikeskus katsoo luonnoksen olevan tarpeellinen ohjeistuskokonaisuus liitteineen, joka tukee julkishallinnon organisaatioita organisoimaan oman poikkeamienhallintansa. Liitteissä erittäin hyvää tukimateriaalia mallipohjiksi.

Seuraavia yleisiä kommentteja kirjattiin:

- Tulisiko määritellä myös tietoturvaloukkaus ja sen ero muihin termeihin, kun sitä ohjeluonnoksessa käytetään?

- Joihinkin ohjeluonnoksen kohtiin, erityisesti kappaleet 4, 4.1 ja 4.2 voisi painottaa tilannetta, jossa kyseessä on vasta tietoturvapoikkeamaepäily ja kuvata yleisiä toimenpiteitä epäilyn vahvistamiseksi tai sen kumoamiseksi

- 'Viranomaisten tulee ilmoittaa havaitsemistaan tietoturvapoikkeamista Viestintävirastolle' vastaava ilmoitusvelvollisuus on tarpeen ja sellainen olisi syytä saada myös säädöstasolle. Ilmoitusvelvollisuutta on kuitenkin tarkennettava mitä eri tietoturvapoikkeamista/-loukkaus-tilanteita se koskee ja koskeeko se myös niistä epäilyjä (erityisesti 2.3. ja 5.3. kappaleissa): Viestintävirastolle ei liene kuulu mm. sisäisien ohjeistuksien rikkomisesta johtuvat poikkeamat, joten tässä voisi miettiä myös eri toimijajoukoille (valtio/kunta/alueellinen/tmv) löytyykö keskitettyä toimijaa jolle olisi syytä ilmoittaa kaikki tietyt poikkeamat esim. valtionhallinnossa on Valtori. Säädöstasolla on tällä hetkellä valtionhallinnossa vain Valtorilla asetuksessaan ilmoitusvelvollisuus valtiovarainministeriölle tai sen osoittamalle viranomaistaholle. Tätä voitaisiin tarvittaessa ohjeistaa Valtorille siten, että Valtori voisi hoitaa ilmoittamisen asiakkaalleen sekä tietyistä poikkeamista tai niiden epäilyistä myös Viestintävirastolle (osa poikkeamista tulee Valtorin tuen kautta esim. loppukäyttäjän ilmoittamana). Lisäksi on huomioitava, että ainakin eri hallinnonaloilla saattaa olla

myös muita sisäisiä määräyksiä tai ohjeita joiden perusteella poikkeamista ilmoitusvelvollisuus voi olla esim. hallinnonalan virastoilta ministeriön suuntaan.

- Kuten ohjeessa sanotaan, usein poikkeamatilanteissa tarvitaan usean toimijan toimia. Tästä syystä olisi hyvä esittää liitteenä esim. mallipohja poikkeamatilanteiden tehtävistä ja vastuista sopimiseksi (esim. RACI-tyyppinen). Se voisi olla yleisimmissä ympäristöistä huomioiden esim.: Valtio: virasto-hallinnonalan_palvelukeskus-Valtori-ulkopuoliset palveluntuottajat sekä jos kuntien osalta on vastaavaa rakenne usein nimettävissä tai vastuita kuvattavissa/suositeltavissa.

- TLP ohjeistus päivittynyt lausuntoaikana:
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/10/ttn201610061413.html

1. Johdanto

Lausuntomme:

Tähän voisi lisätä muita keskeisiä termejä.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Kuvio 2. prosessin kuvassa olevassa pitkässä palkissa 'Viestintä...' tai erikseen vastaava palkki 'Tietoturvatiedon jakaminen' tulisi myös näkyä vrt. ilmoitusvelvollisuus esim. 'tietyistä tietoturvapoikkeamista tai niiden epäilyistä ilmoittaminen sovituille tahoille' sekä harkittavaksi tulisiko sidosryhmät korvata keskeisimmällä sidosryhmillä ja perään vaikka muotoiluksi esim. 'ja muut sidosryhmät'

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

3.1. 'kuka päättää' voisi olla lista asioista 'kuka päättää ja kenen tulee toimia' eli listalle voisi lisätä useampia asioita ja ryhmitellä niitä eri teemojen alle

- Tietoturvapoikkeamiin varautumisesta sekä varautumistoimenpiteistä syntyvistä kustannuksista (tämän voisi katsoa kyllä kattavan kaikki muutkin listalla)

- Tietoturvapoikkeama- tai -loukkausepäilystä

- Tietyistä tietoturvapoikkeamista tai niiden epäilyistä ilmoittaminen sovituille tahoille (huom. per palvelu/palvelutuotantoketju sekä per organisaatio)

- Lisäksi listalla ei ole asioita nostettu havainnointikykyyn taikka seurannan järjestämiseen jota nostaisin esiin, esim. palvelun lokitietojen hallinta ja riskiperusteisesti lokitietojen valvonnan ja analysoinnin järjestämisvastuu. Muutoin on riski siitä, että tietoturvapoikkeamatilanteita havaintaan vain ulkopuolisen siitä ilmoittaessa.

3.1. Taulukko 1 nimessä voisi olla esimerkki ko. organisaation järjestelystä ylätasolla ja toinen taulukko esimerkki organisaation palvelun osalta ml. Palveluntuottaja(t)

3.2. Leviämisen voi laajentaa; 'leviämisen myös muualle valtionhallintoon, julkishallintoon tai laajemmin'.

3.2. Taulukko 2 nimessä voisi olla edessä esimerkki.

3.2. Taulukko 2 säädösviitteet voisi lisätä Henkilötietolain ja Tietoyhteiskuntakaaren pykäliin.

3.3. 'Toisaalta väärin luokiteltu tieto voi myös vaarantaa organisaation tietoturvallisuuden' voisi laajentaa esim. 'Toisaalta väärin luokiteltu tieto voi myös vaarantaa organisaation itsensä ja muiden organisaatioiden tietoturvallisuuden'

3.3.3. voisi lisätä esimerkkejä tapahtumista/poikkeamista mitä Viestintävirastolle ei tarvitse ilmoittaa esim. sisäisten ohjeiden rikkominen, kulunvalvonnan poikkeamat tai ylätasolla vastaavasti.

3.3.8. 'Suomessa tietoturvavaltuutettu' tarkoittaa varmaankin tietosuojavaltuutettua.

3.4.2. Lokitietojen säilytysajoissa voisi mainita muitakin yleisiä vuosilukuja sekä lokitietojen käsittelyn suunnitelmallisuuden, joka on rekisterinpitäjän vastuulla. Esim. virkamiesten käyttämän tietojärjestelmän käyttö- ja auditlokitiedot, jos tietojärjestelmässä toimenpiteillä voi syyllistyä virkarikokseen, olisi perusteltua säilyttää 5 vuotta ko. tapahtumasta.

3.5. Sopimuksien mukaan ilmoittamisessa: tietyistä tietoturvapoikkeamista tai niiden epäilyistä ilmoittaminen sovituille tahoille (esim. asiakasorganisaation tietoturvavastaavalle sekä Viestintäviraston Kyberturvallisuuskeskukselle)

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Seurannan ja valvonnan (ja sen vastuuttamisen sekä resursoinnin) tärkeyttä voisi korostaa jotta tietoturvapoikkeamia voidaan havaita.

4.1. niputtaisin poikkeamatiedon lähteistä yhteen esim. Viestintäviraston ja Valtorin ko. palvelut vaikka alakohtina sekä lisäisin rekisterinpitäjän lainmukaisen käyttöön ja tietosuojan liittyvä seuranta ja valvonta tehtävien suorittaminen sekä palvelutoimittajien tai sidosryhmien yhteydenotot.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

5.1.4. Esimerkkien syvyys vaihtelee ja niiden kuvausrakennetta voisi kehittää esim. taulukoimalla tai otsikoimalla seuraavia yhteisiä tekijöitä esim. Mahdollinen poikkeamatiedon lähde, Tunnusmerkit ja kuvaus, Suositellut toimenpiteet tai varautuminen ja Muuta huomioitavaa (tai siirtämällä lisätieto/laajemmat osuudet kaikista liitteeksi tai laajentamalla niitä).

5.1.4.2. 'murrettu tai saastunut' lisäksi voisi mainita, että laitteiden ja tietojärjestelmien tietyt vikatilanteet tai virhekonfiguraatiot voivat paljastua palvelunestohyökkäyksen lähteeksi.

5.1.4.4. Lisäksi voisi mainita myös henkilökohtaisten ml. sosiaalisen median palveluiden käytöllä sekä tilaratkaisuihin myös etätyö- ja -käyttöperiaatteita ja niiden mukaisia ratkaisuja.

5.3. Lisäksi tulisi välttää spekulointia tai liian varhaisessa vaiheessa tehtäviä johtopäätöksiä.

5.3.x tai 2.3. jompaan kumpaan kohtaan voisi lisätä kappaleen tietyistä tietoturvapoikkeamista tai niiden epäilyistä ilmoittamisesta sovituille tahoille (esim. ko. palvelun tietoturvavastaavalle/asiakasorganisaation tietoturvavastaavalle/organisaatiossa sisäisesti sekä Viestintäviraston Kyberturvallisuuskeskukselle ilmoittamisesta ohjeistusta esim. miten käytännössä turvapostitse vaiko tietyllä lomakkeella) ja erityisesti mistä ilmoittaa ja mistä ei Viestintäviraston Kyberturvallisuuskeskukselle. Samoin voisi rohkaista tietyissä epäilyissä olemaan yhteydessä ja konsultoida KRP:n kyberrikostorjuntakeskusta.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

6.1. Voisi mainita että on syytä kiinnittää erityishuomiota tiettyjen muutosten ja korjausten pikatestauksen järjestämiseen.

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Katso yleiset kommentit esim. tietoturvaloukkaus ja eri termien erot.

Liitteet 2-5

Lausuntomme:

Liite 3. Osin päällekkäistä ohjeen kanssa voisi siirtää tai laajentaa liiteosuutta.

Liite 4. Olisiko status kentässä olevat tiedot kuten poikkeamaepäily/vahvistamatta, vahvistettu poikkeama, korjaustoimenpiteissä oleva poikkeama jne.

Liitteet 6-9

Lausuntomme:

-

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Nämä konkreettisemmat asiat tulisi siirtää asioina tekstiosuuksiin ja mallipohjiin, mutta nk. VAHTI-vaatimuksia on jo aivan liikaa ja aivan eri tarkuustasoilla sekä tietoturvatasoilla. Tietoturvallisuuden hallinnan eri tasoille (tietoturvatasoille) ei suositella asetettavaksi mitään eriäviä vaatimuksia vaan suositeltavaa olisi olla vain pakolliset minimitason julkishallinnon vaatimukset ns. perustasolle.

Ehdotetut perustason vaatimukset ovat

Mahdollista täyttää - vaatii merkittävää toimintamme kehittämistä

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIlle?

-

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Hyvin

Janhunen Kimmo
Oikeusrekisterikeskus