Tampereen kaupunki

Lausunto

10.10.2016

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohje on hyvä ja hyödyllinen.

Teknisenä kommenttina voisi todeta, että otsikoidet fonttien koot olivat epäloogisia ja vaihtelivat eli esim. luvuissa 3.3.1-2 ja 3.3.8 ovat otsikot pienemmällä kuin muut 3.3. alaotsikot ja jossain kohtaa esim. 2. tason otsikot olivat pienemmällä kuin kolmostason jne.

1. Johdanto

Lausuntomme:

-

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

-

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Sivulla 7 Taulukossa 1 käytetyn termin "Virasto" voisi korvata jollain muulla (esim. Organisaation), jolloin ohjeen kyseinen kohta soveltuisi paremmin myös kunnille ja yrityksille.

Sivulla 8. Kohdassa 3.2 todetaan "Tällainen tieto voi liittyä mm. kohdistettuihin tietoturvahyökkäyksiin tai kiristyshaittaohjelmiin, joiden eteneminen valtionhallinnossa voidaan mm. tiedon tehokkaalla jakamisella estää." Koska VAHTI toiminta ja ohje on tarkoitettu koko julkishallintoon, niin tässäkin olisi hyvä tuo "valtionhallinnossa" korvata julkisella hallinnolla ja pyrkiä saamaan näistä asioita tieto/varoitus valtion organisaatioiden lisäksi myös kunnille/kaupungeille. Sama asia myös sivun 9 ensimmäisessä kappaleessa, joissa valtionhallintoon voisi laajentaa julkiseen hallintoon.

Sivulla 16 kohdassa 3.4.1 kohdassa "EU:n tietosuoja-asetus (tulee voimaan vuonna velvoittavana 25.5.2018 siirtymäkauden jälkeen)" on ilmeisesti sana "vuonna" liikaa.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Poikkeaman luokitteluun olisi hyödyllistä sopia jonkinlaiset yhteiset tyypit, joiden mukaan niitä esimerkiksi tilastoitaisiin ja voitaisiin vaikka verrata organisaatioiden välillä. Nykyisellään eri organisaatiot ryhmittelee/luokittelee tietoturvapoikkeamia eri tavoin. Nyt ohjeessa ei ole selkeää luokitusta, jota kaikki voisivat käyttää. Liitteen 7 lomakkeessa on luoteltu muutama tyyppi ja samoin tekstissä kohdan 5.1.4 alla on omat kohtansa muutamille eri tyypeille, mutta olisi hyvä olla jossain "kattava" lista tyypeistä, jota sitten kaikki julkishallinnon organisaatiot käyttäisivät tietoturvapoikkeamien luokitteluun.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

-

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

-

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Kiristyshaittaohjelma (ransomware) kohdassa todetaan "Haittaohjelma, joka salaa kohteen tietoja ja lupaa vapauttaa ne vaadittua lunnasta vastaan." Pitäisikö tuo salaus laittaa esimerkiksi eli on muitakin tapoja kiristää käyttäjää esim. vain sillä, että estetään koneen käyttö jollain muulla tapaa kuin salaamalla tiedostot.

SIRT kohdassa todetaan selitykseksi "Security Incident Response Group Tietoturvatapahtumien hallinnasta vastaava ryhmä.". Eikö tuo T-kirjain tule yleensä tässä yhteydessä sanasta Team eikä Group?

Liitteet 2-5

Lausuntomme:

Liitteen 3 listassa sivulla 35 voisi pari "viraston" sanaa korvata sanalla "organisaation" tai jättää kokonaan pois, jolloin teksti sopii edelleen valtiollekin, mutta paremmin myös kunnille ja yrityksille.

Liitteet 6-9

Lausuntomme:

Liitteen 9 lakilistassa on kaikki lait kahteen kertaan.

Lisäksi listassa voisi huomioida myös kuntia koskevia lakeja.

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Vaatimukset taulukon rivin 19 teksti pitäisi olla osa riviä 18 eikä omalla rivillään.

Rivin 35 vaatimuksen voi käsittää/tulkita useammalla tavalla. Eli viestitäänkö esim. koko henkilöstölle vai vain niille joita poikkeama koskee sekä viestitäänkö aina (pienemmissäkin poikkeamissa) vai vain esim. vakavissa? Se on selvä, että jos laaja ongelma koskee koko henkilöstöä, niin tiedotetaan koko henkilöstölle, mutta jos ongelma koskeekin vain muutamaan työasemaa tai muutaman työntekijän arkaluonteisia tietoja, niin onko tällöinkin tarve tiedottaa koko henkilöstölle? Eli vaatimusta voisi olla hyvä tarkentaa.

Ehdotetut perustason vaatimukset ovat

Mahdollista täyttää - vaatii jonkin verran 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

Koivisto Juha
Tampereen kaupunki