

Asia: VM136:09/2013

## **Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta**

### **Yleistä ohjeeseen liittyen**

#### **Yleiset kommentit ja havainnot ohjeeseen**

Kielen ja ulkoasun tarkistus kannattaa vielä tehdä, ei paljon korjattavaa mutta joitain sanamuotoja pitäisi korjata.

Kaikkiin liitteisiin ei ole viittauksia tekstissä, ainakin liitteeseen 3 olisi hyvä viitata kpl 4.1 – vai onko se vain em. kappaleen toistoa?

### **1. Johdanto**

#### **Lausuntomme:**

-

### **2. Tietoturvapoikkeaman hallintaprosessi**

#### **Lausuntomme:**

Sivulla 5 kuvan yläpuolella vaiheessa 2 puhutaan tietoturvatapahtuman havaitsemisesta ja analysoinnista, kuvan alapuolella puhutaan tietoturvapoikkeamasta.

### **3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen**

#### **Lausuntomme:**

3.1, olisiko syytä määritellä jonkinlainen minimikokoonpano tai roolit, joita ryhmässä pitäisi olla edustettuina?

3.3, numerointi on outo; esim. 3.3.2 puhutaan viranomaisyhteistyöstä ja seuraavissa kappaleissa aletaan luetella yksittäisiä viranomaisia. Kannattaisiko nämä olla kpl 3.3.2 leipätekstissä lueteltuina, ei omina kappaleinaan? Samoin kpl 3.3.11 ja 3.3.12 viestinnän sisälle?

3.3, mainittujen viranomaisten yhteystiedot kannattaisi laittaa liitteeseen tai ainakin linkittää/kertoa mistä ne löytyvät. Erityisesti VIRT on epämääräinen niille, jotka eivät ole olleet toiminnassa mukana.

3.3.2, VIRT = Virtual Incident Security Response Team? Vain onko ... Security Incident ...? Kannattaa tarkistaa myös Liitteen 1 termi.

3.3.5, "Valtiovarainministeriön johtama VIRT-toiminta kehittää julkisen hallinnon vakavien tieto- ja kyberhäiriöiden

operatiivista kyvykkyyttä." Edellisessä lauseessa on jotain vialla. Kehittää häiriöiden operatiivista kyvykkyyttä? Ehkä tarkoitettu häiriöiden hallinnan, selvittämisen tms. operatiivista kyvykkyyttä?

3.3.8, valvova viranomaisella on tietosuojavaltuutettu – todennäköisesti tulee olemaan, tosin sitä ei ole vielä muodollisesti vahvistettu, vaan tehdään kansallisessa lainsäädännössä.

3.3.9, 2. lause, samassa lauseessa puhutaan sekä poikkeama- että häiriötilanteesta.

3.3.9 ja 3.3.12, kannattaa nostaa esille organisaation viestintä-toiminnon rooli – ammattitaitoa kannattaa hyödyntää viestinnän suunnittelussa sekä ulkoisessa viestinnässä, voi parantaa viestinnän selkeyttä ja ymmärrettävyyttä.

3.4.1, miksi viittaus lakiluetteloon on tässä luvussa, se kai koskee ohjetta yleisesti. ei pelkästään lokien keräämistä?

3.5, parempi otsikko olisi ...palveluiden hankinnassa tai ...ulkoistuksissa.

3.5, Puhutaan turvallisuussopimuksesta ja tietoturvaluottamuksesta. Onko oikeasti molemmat vai ainoastaan jompi kumpi?

## 4. Tietoturvaluottamisen havaitseminen ja analysointi

### Lausuntomme:

4.3, mistä luokittelu on otettu? eikä vähäisen ja vakavan välillä ole mitään luokkaa?

## 5. Tietoturvaluottamaan reagointi

### Lausuntomme:

Olisiko loogisempaa rakentaa alaotsikointi kuvan 3 vaiheiden mukaisesti? kannattaisiko esimerkiksi siirtää liitteeseen? Esimerkeistä 8 ja 9 puuttuvat kaikki toimintaohjeet.

5.1.4.3, Väärinkäytön seuraamista ei suositella ilman viranomaisen kehotusta. Mitä viranomaista/viranomaisia tässä tarkoitetaan?

5.3.1, viittaus lukuun 2.3 pitää olla 3.3.

## 6. Toipuminen tietoturvaluottamatilanteista

### Lausuntomme:

Järjestelmien toipumissuunnitelmien lisäksi kannattaa mainita jatkuvuussuunnitelmat, joiden mukaan toiminnot turvataan siinä tilanteessa jos/kun järjestelmät eivät ole käytettävissä.

6.2, viestinnän sisältö luonnollisesti riippuu kohderyhmästä.

## Liite 1. Sanasto

### **Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?**

Onko sanastossa tarpeen olla termejä, joita ei käytetä muualla dokumentissa eikä termien takana olevan teknologian käyttöä avata sen tarkemmin? Esim Honeypot.

## Liitteet 2-5

### **Lausuntomme:**

-

## Liitteet 6-9

### **Lausuntomme:**

Liite 8 ei ole yhteensopiva kpl 5.1.3 lueteltujen tietojen kanssa.

## Vaatimus-Excel ja vaatimukset

### **Palaute, kommentit ja kehittämisideat koskien vaatimuksia**

-

### **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 VAHTIille?**

-

### **Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:**

Hyvin

Miettinen Timo  
Verohallinto