

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Valtiokonttori pitää uutta ohjetta hyvänä ja tarpeellisena, jossa hyvin korostetaan toimimista monitoimijaympäristössä, jossa harva organisaatio kykenee yksin havaitsemaan ja hoitamaan tietoturva- ja muita poikkeamia. Sen vuoksi on tärkeää, että mahdollisimman moni toimija toimii samojen ohjeiden ja mallien mukaisesti.

Ohje on rakenteeltaan selkeä, jossa mennään suoraan asiaan eikä "perinteiseen tapaan" asiaa ensin taustoiteta pariakymmentä sivua. Ohjeen monet selkeät kuviot myös auttavat hahmoittamaan kokonaisuutta.

Vaikka ohje käsittelee tietoturvapoikkeamia, niin myös monien muiden turvallisuus- ym. poikkeamien hallintaan soveltuvat samat ohjeet ja mallit, joten ohjeen alussa voisi tuoda esille myös tämän. Ei ole järkevää, että organisaatio rakentaa erilaisia menettelyjä eri poikkeamien käsittelyyn varsinkaan niiden alkuvaiheessa. Samoin vakavissa häiriö- ja poikkeamatilanteissa on alkuvaiheessa usein vaikea havaita, onko kyseessä tietoturva- vai joku muu poikkeama ja senkään vuoksi eri häiriö- ja poikkeamatilanteiden käsittelyä ei tulisi "liian aikaisin" erottaa toisistaan.

1. Johdanto

Lausuntomme:

-

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

-

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

-

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

4.3. Poikkeaman analysointi: Ensimmäistä kappaletta tulisi muuttaa siten, että kun on varmaa, ettei kyseessä ole tietoturvapoikkeama, asia siirretään toiseen prosessiin eikä jätetä selvittämättä.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Ohjeessa todetaan, että tapahtumapäiväkirja on hyvä rakentaa sähköiseksi palveluksi. Tämäkin palvelu olisi hyvä olla yhtenäinen kaikilla toimijoilla, jonka Vahti voisi tuottaa.

Tähän lukuun voisi myös lisätä selventävän kuvion esim. 2.1 kohdassa olevaa kuviota täydentäen/tarkentaen ottaen mukaan myös luvussa kuvattuja esimerkitapauksia.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

6.4. otsikkoon voisi lisätä, mistä on tarvetta päätöksiä tehdä.

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

-

Liitteet 2-5

Lausuntomme:

-

Liitteet 6-9

Lausuntomme:

-

Vaatus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

-

Ehdotetut perustason vaatimukset ovat

Mielestämme täytämme jo nämä perustason vaatimukset

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIille?

-

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Erittäin hyvin

Pietarinen Juha
Valtiokonttori