

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Poliisihallituksen lausunto VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta ohjeeseen.

Ohje on rakenteeltaan selkeä kokonaisuus, käsittäen poikkeamatilanteiden hallinnan eri vaiheet. Kuvat ja taulukot havainnollistavat hyvin tekstiä. Joiltakin osin tekstin sisältöä olisi selkeytettävä.

1. Johdanto

Lausuntomme:

Määritelmä "Tietoturvatapahtuma" ei ole VAHTI 8/2008 ohjeen mukainen, kun vastaavasti määritelmä "Tietoturvapoikkeama" on.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Kohdassa 2. Tietoturvapoikkeaman hallintaprosessi, tekstin kohdassa 2. on tietoturvatapahtuman havaitseminen ja analysointi, tarkoitettaneen tietoturvapoikkeamaa.

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Taulukon 1 roolijako ei sovellu suoralta kädeltä kaikkiin valtionhallinnon organisaatioihin. Vaatisi hieman tarkennuksia.

3.3.3. Pitäisikö tarkentaa sitä, kuka organisaatiosta ottaa yhteyttä ViVi:n kyberturvallisuuskeskukseen.

3.3.8. Onko meillä "tietoturvaltuutettu", vai onko tämä "tietosuojavaltuutettu".

VIRT -toimintaa voisi kuvata tarkemmin.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Taulukko 4.

Luokitus hyppää vakaavuusasteissa suoraan tasosta "Vähäinen" tasolle "Vakava", olisiko siinä välissä tarve olla yhdelle luokalle.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Kohta 5.1.4.5 Haittaohjelmatilanteet

Pitäisikö tarkentaa kappaleen kolme lausetta "Jos yksi laite havaitaan saastuneeksi, on organisaation tutkittava muidenkin laitteiden mahdollinen

saastuminen". Jos kyseessä on tunnistettu haittaohjelma niin on todennäköistä, että hälytykset tulee kaikista saastuneista laitteista.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Ei kommentoitavaa

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Sanasto tässä yhteydessä käytettäväksi riittävän laaja.

Liitteet 2-5

Lausuntomme:

Pitäisikö liitteen 2. Traffic Light Protocol -luokittelun käyttöä selventää vaikka esimerkeillä.

Liitteen 3 esimerkit ovat hyviä esim. koulutus ja perehdytys käyttöön.

Liitteet 6-9

Lausuntomme:

Liitteiden 7 ja 8 mallit ok.

Liitteessä 9 on samat lait lueteltu kahteen kertaan.

Vaatus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Excelissä on lueteltu varsin mittavat vaatimukset Tietoturvaopikeamien hallintaan jo perustasolla, puhumattakaan korotetun ja korkean tason vaatimuksista. Olisi syytä pohtia näiden vaatimusten suhdetta muihin tietoturvaso vaatimuksiin.

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

Mämmi Ari
Poliisihallitus