

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohje on tarpeeksi laaja-alainen ja selkeä. Ohje ottaa huomioon järjestelmien ja palvelujen ulkoistuksen ja korostaa yhteistyön sekä tiedon jakamisen merkitystä. Hyvää on lisäksi se, että on koottu yhteen vaatimukset tietoturvapoikkeamien hallinnalle perus/korotettu/korkea sekä viittaus vahti ohjeisiin.

Ohje tuo yhtenäisyyttä tietoturvapoikkeamien käsittelylle.

1. Johdanto

Lausuntomme:

Painotettu Viestintäviraston Kyberturvallisuuskeskuksen roolia tietoturvapoikkeamatilanteiden tukemisessa sekä yhteistyön merkitystä muiden organisaatioiden välillä.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Ei lisättävää.

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Kohta 3.1. haastavaa saada perustetuksi tietoturvapoikkeamien käsittelyryhmä/ryhmiä, useita eri järjestelmiä, useita eri toimittajia > resursointi

Kohta 3.4. lokienhallinnan suunnittelu > haastavaa ulkoistetuissa palveluissa

Sinänsä ei lisättävää.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Kohta 4.1. poikkeamatiedon lähteistä > haasteena ulkoistetut palvelut

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

5.1.4.1. > haaste ulkoistetut palvelut/pilvipalvelut > palveluntuottajan havainnot > tieto asiakkaalle

5.1.4.2.> haaste palvelutoimittajan verkkolokit, kuinka saadaan

5.1.4.6 > APT hyökkäys > haaste ulkoistetut palvelut/pilvipalvelut

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Ei lisättävää.

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Ei lisättävää.

Liitteet 2-5

Lausuntomme:

Liitteet 2-5 ok, täydentävät hyvin ohjetta. Ei lisättävää.

Liitteet 6-9

Lausuntomme:

Liitteet 6-9 ok, täydentävät ohjetta. Liitteessä 9 samoja lakeja.

Vaatus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Hyvä, että vaatimukset koottu yhteen.

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?

Hienoa, että tällainen ohje on saatu tehtyä :) otamme käyttöön.

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Erittäin hyvin

Anna-Maarit Kristiina Koivuniemi
ICT -yksikkö/Yhteiset palvelut /tietoturva-asiat