

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohje oli selkeästi etenevä kokonaisuus, jossa tehtiin hyvin selväksi tietoturvapoikkeaman havainnointiin ja käsittelyyn liittyvät toimenpiteet ja vastuutahot.

1. Johdanto

Lausuntomme:

Johdannossa oli hyvin kuvattu ohjeen tarpeellisuus ja avattu käsitteet tietoturvatapahtuma ja tietoturvapoikkeama.

Ensimmäinen lause: "Julkishallinto elää voimakasta muutoksen aikaa." on ehkä hiukan turha, eikä ainakaan kovin aikaa kestävä...toivottavasti.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Ohjeen tässä luvussa on hyvin muodostettu iso kehys ja asia on sen jälkeen pilkottu selkeisiin kokonaisuuksiin. Prosessikuvaus on kattava.

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Käsittelykyvyn muodostaminen organisointineen ja vastuutuksineen on toimiva paketti ns. kustannuspaikkatasolle asti. Luku on kuitenkin ehkä liian laaja ja asiaa olisi toisenkin, erilailla nimetyn luvun alle esim. "Tietoturvapoikkeaman viestintä ja tietoturvatiedon jakelu". Lisäksi tietoturvatiedon jakelusta puhutaan jo ennen kuin varsinaista, asiaa käsittelevää, kappaletta.

Lause:"Tarvittaessa jaettava tieto on hyvä anonymisoida,.. " olisi ehkä parempi muodossa: Jaettava tieto on anonymisoitava seuraavissa tapauksissa...

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Luku oli tiivis ja kattoi hyvin havaitsemiseen ja analysointiin tarvittavat esimerkit ja toimintamallit.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Hyvää ohjetekstiä. Esimerkit poikkeamista voisivat olla myös luvun lopussa.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Kappaleessa oli hyvin tiivistetty toimenpiteet joilla mahdollistetaan toipuminen poikkeamasta. Kappaleen 6.3. nimeäminen: "Raportointi ja tapauksesta oppiminen" voisi olla jotain muutakin. Esimerkiksi "Raportointi ja jatkotoimenpiteet".

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Sanasto on riittävä.

Liitteet 2-5

Lausuntomme:

Liitteet 2-5 ovat toimivia. TLP- luokittelusta kertovassa liitteessä (Liite 2) voisi ehkä alussa kuvata sen käyttötarkoituksen.

Liitteet 6-9

Lausuntomme:

Liitteet 6-9 sopivat hyvin tähän ohjeeseen.

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Vaatimukset ovat kattavat ja sopivat ohjeen henkeen.

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?

Kiitokset hyvästä ohjeesta.

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Erittäin hyvin

Lehtelä Henri
Puolustushallinnon rakennuslaitos