Opetushallitus

Lausunto

06.10.2016 37/050/2016

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohje on erittäin toivottu ja tarpeellinen havaintojen luokittelun ja niiden perusteella päätettävien toimenpiteiden takia.

1. Johdanto

Lausuntomme:

Tavoitteet tulevat selville. Ei lisättävää.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Selkeyttäisin hallinnan päävaiheita ja operatiivista käsittelyprosessia. Nyt "Tietoturvapoikkeamien käsittelykyvyn muodostaminen" on hallinnollinen vaihe, mutta muut hallinnan vaiheet enemmän operatiivisia, joita tarkentaa käsittelyprosessin kuvaus. Yleisissä malleissa "käsittelykyvyn muodostaminen" ymmärretään yleensä tietoturvapoikkeaman hallinnalla (management). Voisiko prosessiin ottaa mukaan hallintavaihe omanaan kuten tässä: https://nigesecurityguy.files.wordpress.com/2013/06/vulnerability-process.jpg ja tuo "Tietoturvapoikkeamien käsittelykyvyn muodostaminen" vaikka läpileikkaavaksi prosessiksi?

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Käsittäisin "Käsittelykyvyn muodostaminen" vaihetta enemmän varautumisen ja operatiivisin toiminnan yleisellä hallinnatamallilla (governance) ei varsinaisena tietoturvapoikkeaman operatiivisella hallinnalla (management). Tämä sinänsä hyvä, mutta havainnon osalta operatiivisen hallinnan (management) ohjeet pitäisi olla myös selkeät. Käsittelykyvyn muodostaminen on ok sinänsä, mutta sen rooli on erilainen.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Tähän voisi muistuttaa tarkemmin käsittelyyn liittyvistä juridisistä vastuista esim. henkilötietojen osalta (edit. 5.1.4.4 kappaleessa onkin mainittu). Luokitteluun voisi liittää mukaan maininnan, että havainnon luokittelu kannattaa sovittaan organisaation omaan riskienarviointikehikkoon (taloudellisen, maine yms kriisien vaikutukset toimintaan).

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

"5.1.4.4 Oman henkilökunnan tekemät tietoturvaloukkaukset" tähän voisi vielä tarkentaa esimerkillä, ettei esimerkiksi käyttövaltuuden eväämistä virkamieheltä tietoturvaepäilyjen johdosta voida tehdä ilman asiaan liittyviä juridisia varmistuksia.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Vaiheeseen kuuluu päätöksenteko sisäisesti. Jos pääprosessiin otetaan mukaan management niin se kattaa myös tämän vaiheen päätöksentekoprosessin

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

-

Liitteet 2-5

Lausuntomme:

onko TLP luokittelusta oikeasti hyötyä kun tavoitteena on ollut vähentää luokittelua ylipäätään? Toki kannattaa yleisesti noudattaa kansainvälisiä luokitteluja

Liitteet 6-9

Lausuntomme:

Hyviä malleja. Liite 9:n lainsäädännöstä voisi nostaa esimerkkejä ja viittauksia itse ohjetekstiin, jotta ohjeen perusteella osaa suoraan huomioida juridiset asiat

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Vahti vaatimusviitteen (mistä tulee) voisi lisätä taulukkoon.

"Organisaatiolla on käytettävissä kriittisten poikkeamien hallintaan liittyvät johtamistilat" on vähän keinotekoinen vaatimus ja käsittely voi olla sähköisessä ympäristössäkin.

"Organisaatiolla on tietoturvapoikkeamien hallintaan liittyvät viestintävälineet" Ei sinänsä kerro mitään

Organisaatiolla on SIEM on kova vaatimus, mutta toki toimii suosituksena

Ehdotetut perustason vaatimukset ovat

Mielestämme täytämme jo nämä perustason vaatimukset

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIlle?

Tässä on nyt hyvää konkretiaa mitä on toivottu uusilta Vahti-ohjeilta

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Hyvin

Keränen Esa
Opetushallitus - Opetushallitus