

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Helsingin kaupungin lausunto ohjeesta VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Ohje tuo hyvin esille kuinka vaativaa toimintaa on tietoturvapoikkeamien hallinta sekä siihen oleellisesti liittyvä tieto- ja viestintäkyvykkyyden jatkuvuuden hallinta. Hyvän, ympärivuorokautisen tietoturvapoikkeamien hallintakyvyn saavuttaminen vaatii merkittävää työpanosta, osaamista ja myös teknisiä tukijärjestelmiä.

Digitalisaation edetessä jatkuvasti suurempi osa kunnan palveluista on saavutettavissa kellon ajasta riippumatta. Ja nekin kunnan palvelut, joita käytetään normaalina työaikana, vaativat ympärivuorokautista ongelmiin reagointikykyä. Vaikka laiterikko, järjestelmään tunkeutuminen tai muu häiriö sattuisikin viikonloppuyönä, niin silti seuraavalla arkipäivän työvuorolla järjestelmää ja sen tietoja taas tarvitaan.

Tämä ohje antaa hyviä käytännön toimintamalleja tietoturvan laatupoikkeamien hallintatyölle. Ohjeesta nousee esille myös tarve tietoturvatiedon jakamisen tekniselle ympäristölle.

Korkean turvallisuuden ja korkean käytettävyyden tieto- ja viestintäjärjestelmien tulisi olla osa kunnalle tarjottavia normeja arjen tieto- ja viestintäratkaisuja. Tällöin sellaisen käyttö olisi normaaliajan perustoimintaa ja olisi kunnan tietojen käyttäjälle helposti omaksuttava. Kuntien laajasti käyttämät korkean turvallisuuden ja käytettävyyden normaaliajan tieto- ja viestintäjärjestelmät tukisivat kansallista kyberturvallisuutta erittäin merkittävästi. Iso osa kansalaisten, yritysten ja yhteisöjen toimintaa tukeutuu toimivaan kuntaan.

1. Johdanto

Lausuntomme:

Johdannon esittämään lähtökohtaan on helppo yhtyä. Kuntien digitalisaatio ja monitoimittajaratkaisut vaativat kaikilta palvelun tuotantoon osallistuvilta kykyä tietoturvan (kyberturvan) vaalimiseen.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Esitetty kuvaus tietoturvapoikkeamien hallinnasta on pätevä. Prosessin vuokaavio jäsentää hyvin kuinka vaativasta asiasta on kyse.

Maininta rikosilmoitusprosessiin liittymisestä voisi sopia jo tähänkin kappaleeseen.

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Tietoturvapoikkeamien käsittelyn organisoinnin kuvaus auttaa ymmärtämään, että kyvykkyyden saavuttaminen vaatii laajasti henkilöstön työpanoksen kohdentamista ja osaamiseen sijoittamista.

Menettelyjen periaatteet soveltuvat myös kuntatoimijalle, vaikkakin tekstissä puhutaan valtionhallinnasta. Tietoturvatiedon luokittelua kuvaava taulukko auttaa hyvin asian jäsentämistä.

Taulukko tietoturvapoikkeamien ilmoittamisesta alleviivaa tehokkaasti millaisia reagoitukykyjä tavoitellaan. Kunnissa ja kunnille tieto- ja viestintäpalveluita tuottavissa palvelutoimittajissa tullaan tarvitsemaan merkittäviä panostuksia, jotta kuntien digitalisaatiosta välttämättä seuraavat laatu-poikkeamien hallinnan reagoitukyvyt saadaan taulukossa esitetyille tasoille.

Yksityiskohtana voisi kappaleessa 3.3.7 mainita mikä ja missä toimii Suomen kansallinen turvallisuusviranomaisen.

Teknisenä huomiona kappaleen 3.3.9 otsikkotyö on luonnoksessa italics muista kappaleen samantasoisista otsikoista poiketen.

Kappaleessa esitetyt viestinnän, lokihallinnon, palvelusopimusten ja poikkeamatilanteiden harjoittelun tarpeet kuvaavat hyvin kuinka vaativasta toiminnasta on kokonaisuudessaan kyse.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Esitetty kolmitasoinen poikkeaman vakavuusasteen luokittelu (vähäinen, vakava, kriisitilanne) tuntuu käytännölliseltä lähtökohdalta ongelmaan reagoinnin tarvetta tunnistettaessa.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Kappaleessa esitetyt esimerkit erilaisilta poikkeamatilanteista antavat hyvän kuvan kuinka erilaisia reagointia vaativat tilanteet ovat. Samalla kappaleessa tuodaan hyvin esille se, että onnistuva poikkeamiin reagointi vaatii organisaatiolta riittävää henkilöstöä sekä johtamaan että suorittamaan käytännöllisiä toimenpiteitä. Organisaation, joka pyrkii tällaisen kyvyn rakentamaan, on tehtävä merkittävä investointi työpanokseen, osaamiseen ja tarvittaessa myös teknisiin järjestelmiin.

Kuntien tietoturvatiedon jakamista tukisi, jos tarjolla olisi valmiiksi tällaista varten rakennettuja tiedonjakopalveluita. Korkeaa turvallisuutta ja korkeaa käytettävyyttä vaativien teknisten tieto- ja viestintäjärjestelmien toteuttaminen on kallista, vaatii palvelutoimittajalta erityisosaamista ja voi muodostua hinnaltaan liian kalliiksi markkinaehtoisille toimijoille. Siksi kuntatoimijoiden voisi olla mielekkäintä hankkia tällaisia erillispalveluita niihin erikoistuneilta palvelutoimittajilta.

Tällaisen tietoturvatiedon jakamisen ympäristön tulisi olla osa normaalia arjen tieto- ja viestintäratkaisujen tarjontaa. Tällöin sen käyttö ei vaadi erityisiä ponnisteluja ja omaa, muusta arjesta irrallista työskentelytapaa. Normaaliajan perustoimintaan liittyvä korkean turvallisuuden ja korkean käytettävyyden tieto- ja viestintäjärjestelmä olisi oltava kunnan tietojen käyttäjälle helposti omaksuttava. Sellainen tukisi perustavaa laatua olevalla tavalla kansallista kyberturvallisuuden tavoitetta.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

Kappale vetää yhteen riittävällä tavalla poikkeamatilanteen loppuselvittelyn viitaten samalla jatkuvuuden hallinnasta tuotettuun omaan VAHTI-ohjeeseen. Tämä liittyy hyvällä tavalla jatkuvuuden hallinnan ja poikkeamien hallinnan yhdeksi, laajaksi osaamiskokonaisuudekseen.

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

Tällaisessa ohjekirja muotoisessa julkaisussa ohjekohtainen sanasto on oikein hyvä olla olemassa. Tietoturvan (kyberturvan) erityissanastojen verkkojulkaisuissa voisi olla yleisöä palvelevaa saada tarvittavat termit osaksi yleisesti saatavia sanastoja, kuten esimerkiksi Sanastokeskus TSK ry:n sanastoihin.

Liitteet 2-5

Lausuntomme:

Traffic Light Protocol –luokittelu antaa hyvän mallin tietojen jakelutoiveiden esittämisestä, kun lähettäjä tahtoo rajata tietojen kohderyhmää. Esimerkkinä voisi laittaa vaikka kuinka sähköpostin otsikkotiedoissa lähettäjä voisi näitä käyttää. Liitesivulle voisi myös laittaa viittauksen verkkolähteeseen, mistä löytyy taustaa mitä TLP-luokittelu on ja mistä se tulee.

Esimerkit poikkeaman ilmenemisestä, havaintojen keräämisestä ja viestinnästä tuovat ohjeessa esitetyt asioita hyvällä tavalla lähemmäksi käytännön arkityötä.

Liitteet 6-9

Lausuntomme:

Esimerkit poikkeamatilanteen hallinnan ohjeistamisesta, ilmoituslomakkeesta sekä tapahtumien kirjaamisesta antavat lukijalle hyvän lähtökohdan ymmärtää kuinka paljon osaamista ja tekemistä onnistuva poikkeamanhallinta vaatii.

Lakikooste antaa riittävän mielikuvan siitä, että myös kunnalle on lakiperusteita kyetä hallitsemaan tieto- ja viestintäjärjestelmiin ja tietoihin itsessään kohdistuvat laatu-poikkeamat.

Erityisesti kuntien toimintaan kohdistuvista lakivelvoitteista voisi olla hyödyllistä koota oma luettelonsa esimerkiksi kuntien eri toimialoihin jakautuen. Kullakin kunnan toimialalla tai palvelukokonaisuudella on omaa lainsäädäntöä, joista voi löytää perusteluja kunkin toiminnan vaatimiin erityisjärjestelyihin. Tällainen kaikkien kuntien yhteisiä lakivelvoitteita kuvaava luettelo voitaisiin tuottaa ohjeen julkaisun jälkeen joillain sopivilla kuntien lakipalveluiden, tietosuojan tai tietoturvan (kyberturvan) yhteistyöfoorumeilla.

Vaatus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Taulukko auttaa ymmärtämään kuinka vaativasta toiminnasta on kyse, kun pyritään hyvään poikkeamienhallintaan. Viitteet muihin VAHTI-ohjeisiin auttavat tunnistamaan kuinka laaja osa-alue tietoturvan (kyberturvan) johtaminen ja käytännössä toteuttaminen on.

Ehdotetut perustason vaatimukset ovat

Mahdollista täyttää - vaatii merkittävää toimintamme kehittämistä

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIille?

Tällaiset tiettyyn teemaan liittyvät ohjekirjat soveltuvat erinomaisen hyvin asioiden järjestelmälliseen oppimiseen kunnassa ja kuntien palvelutoimittajissa. VAHTI-ohjeet auttavat yhdenmukaistamaan tietoturvan laatua tieto- ja viestintäjärjestelmissä, palvelutoimittajien toiminnassa sekä kuntien omassa toiminnassa.

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

Hyvin

Aaro Antero Hallikainen
Helsingin kaupunki

