Kehitys ja laatu / Tommi Simula

21.10.2016

Lausunto luonnokseen VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallintaohje

Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) on 16.9.2016 pyytänyt lausuntoa aiheesta Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta. Tämä lausunto kattaa Valtion tieto- ja viestintätekniikkakeskus Valtorin keräämät lausunnot aiheeseen.

1 Yleiset kommentit

Tietoturvapoikkeamien hallinnan merkitys on viime vuosina korostunut entisestään, ja toimiva yhteistyö ja tiedottaminen häiriötilanteissa on ensisijaisen tärkeää. Valtionvarainministeriön ja Kyberturvallisuuskeskuksen tekemä työ aiheen osalta on ollut erittäin arvokasta, ja toivomme työn ja osa-alueen yhteisten käytäntöjen kehittämisen jatkuvan.

Esityksenä toteutettavaksi keskitetty tietoturvallisuuden poikkeamatietokantapalvelu, johon virastojen tietoturva-asiantuntijoilla on pääsy tietojen ylläpitoa ja esiintymien tarkastelua varten. Tietokannasta saisi mahdollisimman tarkkaa tietoa esiintyvistä tietoturvaongelmista ja siitä voidaan nostaa esiin hakuotannoilla selkeitä puutteita tai trendejä. Ratkaisu auttaisi koordinoimaan valtionhallinnon tietoturvaa ja löytämään heikot kohdat, jotka toistuvat virastoittain. Palveluun tallennettava tieto tulisi anonymisoida, sekä mahdollisesti tallentaa riittävällä viiveellä itse tapahtumien jälkeen, jotta tarvittavat korjaukset ja kontrollit ehditään muualla valtionhallinnossa toteuttaa.

Kokonaisuutena ohjeluonnos vaikuttaa kattavalta ja hyvin valmistellulta.

2 Ohjeluonnos VAHTI_luonnos_03_2016_tietoturvapoikkeamien_hallinnan_ohje_1409_2016

2.1 Tietoturvapoikkeamien hallintaprosessi

Luvussa 2 esitetään tietoturvapoikkeamien hallintaprosessiin liittyviä malleja ja esimerkkejä. Yksi käytännön osoittama haaste on poikkeamatapausten luokittelu ja tietoturvapoikkeamien tunnistaminen. Lähes kaikki häiriöt ja poikkeamat tunnistetaan aluksi toiminnallisiksi häiriöiksi, ja niiden oikea luokittelu tietoturvapoikkeamaksi vaatii työtä ja osaamista. Monesti organisaatioilla on omat vastuut ”tavallisten” palvelujen tai toiminnan häiriöiden hallintaan, sekä erilliset vastuut tilanteisiin, jotka luokitellaan tietoturvapoikkeamiksi. Tämä johtaa usein viiveisiin, epäselviin vastuihin sekä päätöksiin vajavaisilla tiedoilla.

Valtorin näkemyksen mukaan ideaalitilanteessa tietoturvapoikkeamien hallinta on osa normaalia häiriöhallintaa, eikä poikkeamatyyppi muuta tilanteen selvittämisen tai viestinnän vastuita. Tietoturvapoikkeamat

vaativat kuitenkin erityisosaamista sekä tietyissä tapauksissa rajoittavat tai ainakin muuttavat tilanteissa tehtävää tiedottamista ja raportointia, joten tarvittavien resurssien saaminen mukaan selvitystyöhön sekä operatiivinen ohjeistus näiden tilanteiden varalta on tietysti välttämätöntä. Kuitenkin sillä, että poikkeaman selvitys- ja tiedostusvastuut poikkeamatyypistä riippumatta ovat aina samoilla rooleilla selkeytetään tilanteiden vastuita, sekä estetään ns. vastuiden pallottelu organisaation sisällä sen mukaan mihin kategoriaan poikkeama missäkin selvitystyön vaiheessa katsotaan kuuluvan.

Ohjeessa tulisi siis ehkä tuoda esiin suositus siitä, että tietoturvapoikkeamat hallinnoidaan organisaatioissa samoin prosessein ja vastuin kuin muutkin toiminnalliset häiriöt ja poikkeamat, mutta selvitysryhmää tarvittaessa vahvistetaan tarvittavilla tietoturvallisuuden resursseilla, sekä tietoturvapoikkeamien mm. tiedotukseen, viestintään, salassapitoon ja viranomaisyhteistyöhön liittyvät asiat kuvataan omaan ohjeistukseensa. Ohje voisi myös sisältää esimerkin siitä, miten tietoturvapoikkeamien käsittelyn erityisvaatimukset integroidaan esim. ITIL-prosesseihin. Tällä myös osaltaan pyritään välttämään mielikuvaa siitä, että tietoturvapoikkeamien käsittely tai tietoturvallisuus ylipäätään ovat jotenkin organisaation linjatyön ulkoista toimintaa, jonka vastuut eivät liity työntekijöiden normaaliin työhön.

Luvussa 3.3. määritellään ensin tietoturvatiedon jakamisen ja viestinnän ero. Alaluvussa 3.3.1 käsitellään tt-tiedon jakamista, mutta sitten seuraavissa alaluvuissa määritellään tiedon jakamiselle olennaiset tahot. Vasta alaluvussa 3.3.9 palataan taas viestintään. Tätä ryhmittelyä tai jäsentelyä voisi selkiyttää.

Sisällysluettelo on sekaisin ja/tai useita lukuja puuttuu (esim 3.3.3.-3.3.8.). Lisäksi luvussa 5.3.1 viitataan täysin olemattomiin lukuihin 4.3.1 ja 2.3.

Luku 5.3.2 Viestintä reagoinnin aikana puhuu välillä tiedon jakamisesta, välillä tiedottamista ja välillä viestinnästä. Lukua 5.3. olisi vielä syytä tarkentaa ja lukea sitä verraten luvun 3.3. kanssa.

2.2 Tietoturvapoikkeamien käsittelyn organisointi

Kappaleessa 3.1 esitetään suositukset hallintaryhmän kokoonpanolle. Esityksessä voisi ottaa vielä tarkemmin kantaa toimi- ja päätösvaltakysymyksiin. Ryhmällä tulee olla riittävä päätäntävalta yleisimpien kontrollikeinojen toimeenpanolle, ja nämä voisi olla hyvä esim. palvelu- tai prosessikohtaisesti määrittää etukäteen. Yhtenä esimerkkinä voisi käyttää vaikka sitä, että ryhmällä on valta päättää esim. poikkeaman kohteena olevan palvelun väliaikaisesta alasajosta, ja varmistaa, että mandaatti tälle löytyy.

Taulukkoon yksi voisi lisätä optionaalisena mukaan organisaation lakiosaston edustuksen, jotta voidaan arvioida tarkasti tehtävien päätösten juridiset tai sopimusvaikutukset.

3 VAHTI_luonnos_03_2016_poikkeamanhallinta_vaatimukset_1409_2016

Luonnos sisältää 38 kappaletta vaatimuksia, joista perustasoa koskevia pakollisia vaatimuksia on 24 kappaletta. Suosittelisin vielä käymään asetetut vaatimukset tiheällä kammalla läpi arvioiden niiden vaikuttavuutta ja toteuttamisen sekä toteuttamisen valvonnan kustannuksia, sekä päällekkäisyyksiä jo määriteltyjen vaatimusten kanssa. Vaatimusten tulee kuitenkin määrittää asetettu minimitaso, joka on kustannustehokkaasti toteutettavissa kaikissa valtionhallinnon organisaatioissa, ei tavoiteltavaa optimitasoa turvallisuuskriittisissä ympäristöissä.

Oheen nostettuna esimerkinomaisesti vaatimuksia, joiden tarkoituksenmukaisuutta pyytäisin erityisesti arvioimaan:

Vaatimus	Kommentit
Organisaatio on asettanut tietoturvapoikkeamien käsittelyryhmän, jonka kokoonpano voi vaihdella poikkeaman vakavuuden perusteella	Onko ryhmän nimeäminen välttämätöntä? Pitäisin olennaisena, että selvitysvastuut on määritelty, sen miten selvitystyö on organisoitu katsoisin olevan toissijaista.
Organisaatio on määrittänyt tietoturvapoikkeamien käsittelyvastuut	Päällekkäinen 2/2010 kanssa
Organisaatio on määrittänyt tietoturvapoikkeamien päätöksentekovaltuudet	Ehdottomasti suositeltavaa, mutta onko varmasti välttämätöntä kaikissa organisaatioissa?
Organisaatio on määrittänyt vastuutahon ja menettelytavat tietoturvapoikkeaman ilmoittamisesta vastuuviranomaisille	Päällekkäinen 2/2010 kanssa
Organisaatiolla on käytettävissä kriittisten poikkeamien hallintaan liittyvät johtamistilat	Vaatimuksella oletettavasti tavoitellaan poikkeamatilanteissa käytettyjen tietojen käsittelyn suojaamista. Edellyttääkö tämä aina erityisiä johtamistiloja?
Organisaatiolla on tietoturvapoikkeamien hallintaan liittyvät viestintävälineet	Voisiko mieluummin määrittää, että poikkeamien hallintaan käytettävistä viestintävälineistä on sovittu? Pitäisin kuitenkin enemmän suosituksena kuin pakollisena vaatimuksena, kaikilla organisaatioilla on kuitenkin jo pakollisena luokiteltujen tietojen käsittelysäännöt ja -ohjeet tietoturvatasojen vaatimuskohdan 1.5.1 nojalla.

Organisaatiolla on tietoturvapoikkeamien hallintaan tarvittaville tiedoille ja dokumenteille keskitetty säilytyspaikka	Keskitettyä säilytyspaikkaa en pitäisi pakollisena vaatimuksena millään tasolla. Keskitetty sijainti, josta löytyy tiedot mitä tietoja ja dokumentteja aiheeseen liittyy voisi olla kuitenkin hyvä suositus.
Sopimuksessa on määritelty tietoturvapoikkeamien käsittelyn ja tiedon jakamisen toimintamallit	Toimintamallien kuvaus perustasolla kaikissa sopimuksissa kuulostaa liialliselta. Pitäisin olemassa olevia vaatimuksia tämän osalta riittävänä (Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.)
Organisaatio kannustaa henkilöstöä ilmoittamaan tietoturvapoikkeamista	Pitäisin ympäripyöreänä ja mahdottomana mitata, selkeästi suositus, ei vaatimus.
Organisaatio viestii poikkeamasta henkilöstölle ja sidosryhmille	Vaatimus ristiriidassa salassapitovelvoitteiden ja rikostutkinnan vaatimusten kanssa. Yleisemmän tason laajempi tiedottaminen eisensitiivisten tietojen osalta varmasti erittäin suositeltavaa, mutta en näe poikkeamien selvittämisen näkökulmasta pakollisena.
Organisaatio jakaa poikkeamatietoa sisäisten ja ulkoisten sidosryhmien kanssa	Kuten edellä. VM:n tulee määrittää tarkasti velvoitteet mistä poikkeamista ja mitä tietoja on pakollista jakaa ja kenelle.
Palvelusopimuksissa toimittaja on velvoitettu valvomaan tietojärjestelmien tietoturvallisuutta	Tässä pitäisi määritellä mitä tarkkaan ottaen tarkoitetaan valvonnalla ja mitä tietojärjestelmiä. Mikä on riittävää valvontaa esim. runkoverkkopalvelun, sähköpostipalvelun tai pilvestä tuotettavan sovelluksen osalta? Mikäli vaatimusta ei tarkenneta, sen toteutumista ei voida auditoimalla varmentaa. Jos tarkennetaan, se hyvin suurella todennäköisyydellä aiheuttaa merkittäviä lisäkustannuksia sopimuksiin myös tilanteissa joissa se ei ole tarkoituksenmukaista. Suosittelisin muuttamaan suositukseksi.
Organisaatiolla on ajantasaiset varmistukset tiedoista ja järjestelmistä	Mitä tarkoitetaan ajantasaisella, mistä tiedoista ja järjestelmistä? Monissa järjestelmissä ajantasaisten varmistusten ottaminen on tarpeetonta (tiedot staattisia tai helposti uudelleen rakennettavissa). Mielestäni vaatimus on myös poikkeamahallinnan skoopin ulkopuolella.

Helsingissä 21.10.2016

Tommi Simula
Riskienhallintapäällikkö