26.9.2016

Valtionhallinnon tieto- ja kyberturvallisuuden
johtoryhmä (VAHTI)

Keskusrikospoliisin lausunto ohjeluonnoksesta VAHTI 3/2016; Tietoturvapoikkeamatilanteiden hallinta sekä vaatimuksista tietoturvapoikkeamanhallinnalle

Valtiovarainministeriön Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) on pyytänyt Keskusrikospoliisilta lausuntoa ohjeluonnoksesta VAHTI 3/2016; Tietoturvapoikkeamatilanteiden hallinta sekä luonnoksesta vaatimuksiksi tietoturvapoikkeamanhallinnalle eri tietoturvallisuuden tasoilla. Lausunto tuli antaa viimeistään maanantaina 10.10.2016. Lausunnot pyydettiin antamaan sähköisen lausuntopalvelun kautta, mikä vaatii rekisteröitymisen. Keskusrikospoliisi antaa virallisen lausuntonsa tästä poiketen tässä asiakirjassa.

Keskusrikospoliisi pitää lausunnolla olevia luonnoksia lähtökohtaisesti kannatettavina ja perusteltuina. Yhteiskunnan nopeasti muuttuessa entistä tietoteknisemmäksi toimintaympäristöksi, on tärkeää varmistaa yhdenmukaiset mekanismit tietoturvapoikkeamiin varautumisessa, niihin reagoimisessa sekä niistä toipumiseen. Keskusrikospoliisi kiinnittää kuitenkin huomiota seuraaviin luonnoksissa oleviin kohtiin.

LAUSUNTO

Ohjeluonnos VAHTI 3/2016; Tietoturvapoikkeamatilanteiden hallinta

Kohta 2. Tietoturvapoikkeaman hallintaprosessi

Johdannossa sivulla 4 on määritelty tietoturvatapahtuma ja tietoturvapoikkeama. Tähän perustuen sivulla 5 voidaan päätellä olevan asiavirhe. Tietoturvapoikkeaman hallintaprosessi on jaettu ohjeessa neljään päävaiheeseen. Toisessa kuvatussa vaiheessa käytetään tietoturvatapahtuman käsitettä, kun taas tätä selventävässä tekstissä samalla sivulla käytetään tietoruvapoikkeaman käsitettä.

Kohta 3.3.3 Viestintäviraston Kyberturvallisuuskeskus

Ensimmäisessä kappaleessa tietoturvapoikkeaman havaitsemisen jälkeen pyydetään ottamaan ensisijaisesti yhteyttä Viestintäviraston Kybertuvallisuuskeskukseen.

Keskusrikospoliisin näkemyksen mukaan kohtaa tulisi tarkentaa yhteydenoton suhteen eli kenelle organisaatiossa kuuluu viime kädessä yhteydenoton tekeminen. Ohjeesta saa käsityksen, että kuka tahansa organisaatiosta voi tehdä yhteydenoton, jolloin tiedonkulku organisaation sisällä voi jäädä vajaaksi. Ohjeessa tulisikin ainakin viitata organisaation virallisiin prosesseihin yhteydenoton suhteen tiedonkulun varmistamiseksi. Lausunnolla olevissa tietoturvapoikkeamanhallinnan vaatimuksissa tämä on kuitenkin otettu asianmukaisesti huomioon.

Kohta 3.3.4 Poliisi

Ensimmäisessä kappaleessa todetaan, että mikäli havaituissa tietoturvapoikkeamissa epäillään rikosta, on aina syytä tehdä rikosilmoitus. Rikosilmoitus tehdään paikallispoliisille, josta asia tarvittaessa siirretään Keskusrikospoliisin tutkittavaksi.

Keskusrikospoliisi korostaa, että rikosilmoitus on aina syytä tehdä mahdollisimman nopeasti. Tekstiä voisi tarkentaa myös siltä osin, että tarvittaessa rikosilmoitus siirretään paikallispoliisista Keskusrikospoliisin Kyberrikostorjuntakeskuksen tutkittavaksi. Kyberrikostorjuntakeskus voi antaa myös neuvoja jo ennen rikosilmoituksen tekemistä tai sen yhteydessä siitä, millä tavoin todistusaineisto turvataan kyseisessä tapauksessa taikka muista tapaukseen liittyvistä seikoista.

Kohta 3.5 Tietoturvapoikkeamien huomioiminen sopimusmenettelyssä

Kolmannessa kappaleessa mainitaan esimerkkinä haasteet pilvipalvelujen käytössä ja siitä sovittaessa turvallisuussopimuksessa. Pilvipalvelut ovat jatkuvasti kasvavassa asemassa tietoyhteiskunnassa. Pilvipalveluihin liittyviä haasteita voitaisiin Keskusrikospoliisin näkemyksen mukaan avata enemmän myös tässä ohjeessa. Olisi tarpeellista todeta ainakin ne vähimmäisvaatimukset, jotka pilvipalveluja käytettäessä olisi otettava tietoturvapoikkeamina huomioon.

Pilvipalvelut liittyvät vahvasti myös eri maiden lainsäädännöllisiin eroihin, mikä korostaa pilvipalvelujen ohjeistamista ohjeessa tarkemmin. Ohjeistaa voitaisiin myös se, milloin sopimus tulisi jättää tekemättä kokonaan. Pilvipalvelut voisivat olla myös kohdassa 5.1.4 esimerkkinä erilaisista poikkeamatilanteista, kuten riskinä tietojen joutumisesta ulkopuolisen hallintaan tai erilaisista tietoihin liittyvistä kiristyshaittaohjelmista. Asian merkitys korostuu erityisesti organisaatioissa, joissa käsitellään mitä tahansa salassa pidettävää tai muutoin luottamuksellista tietoa.

5.1.2 Poikkeaman lähteen selvittäminen

Kappaleessa todetaan, että mikäli selviää tai epäillään rikosta, on poikkeaman lähteen selvittäminen poliisin tehtävä.

Keskusrikospoliisi korostaa tässäkin yhteydessä, että poliisille tulisi ilmoittaa rikosepäilyn kyseessä ollessa mahdollisimman varhaisessa vaiheessa sekä turvata poliisille mahdollisimman autenttiset edellytykset poikkeaman selvittämiseen.

5.1.3 Tapahtumapäiväkirjan pitäminen

Ensimmäisessä kappaleessa todetaan, että tietoturvapoikkeamien käsittelyssä tehtävät havainnot, päätökset ja toimenpiteet on kirjattava tapahtumapäiväkirjaan samalla, kun niitä tehdään.

Ohjeessa voitaisiin Keskusrikospoliisin näkemyksen mukaan korostaa dokumentaation laatimisen ohella sen huolellista säilyttämistä. Dokumentaatio voi olla tärkeä tekijä myös poliisille, mikäli tietoturvapoikkeamaa tutkittaisiin myöhemmin rikoksena.

5.3.2 Viestintä reagoinnin aikana

Ensimmäisessä kappaleessa todetaan, että poikkeamasta on syytä viestiä ennen kuin virheellisiä tai puutteellisia tietoja alkaa levitä muuta kautta.

Keskusrikospoliisi korostaa, että esitutkintalain 11 luvun 7 §:n 4 momentin mukaan oikeus antaa esitutkinnasta tietoja julkisuuteen on tutkinnanjohtajalla ja hänen esimiehillään sekä heidän määräämällään muulla virkamiehellä. Oikeus tietojen antamiseen on myös syyttäjällä esitutkinnan päättymisen jälkeen.

Liite 7. Tietoturvapoikkeaman ilmoituslomakkeen malli

Keskusrikospoliisin näkemyksen mukaan lomake voisi olla ohjaavampi tai lomakkeeseen tulisi liittää tarkentava ohjesivu. Esimerkiksi lomakekohta 'kokemuksesta oppiminen' voi jäädä lomaketta täyttävälle epäselväksi ilman kuvausta tarkoitetusta asiasta.

Liite 8. Tapahtumapäiväkirjan malli

Keskusrikospoliisin näkemyksen mukaan tapahtumapäiväkirjamallissa voisi olla yhtenä sarakkeena poikkeaman vakavuutta kuvaava merkintä esimerkiksi numerollisena arviona. Merkintä kuvaisi selkeästi poikkeaman vakavuutta ja tarvittavien toimenpiteiden merkitystä. Lisäksi lista todistusaineistosta olisi selkeämpää kirjata taulukkomuotoon yksilöityihin tietosarakkeisiin, joita olisivat esimerkiksi päivämäärä, havainto ja tehdyt toimenpiteet.

Liite 9. Tietoturvapoikkeamien hallintaan liittyvä lainsäädäntö

Liitteessä on lueteltu samat säädökset kahteen kertaan.

Keskusrikospoliisin näkemyksen mukaan ohje soveltuu hyvin käytettäväksi organisaatioiden tietoturvapoikkeamien käsittelyyn.

Vaatimukset tietoturvapoikkeamanhallinnalle v.0.82

Tietoturvapoikkeamien käsittely ja torjunta otsikoidussa kohdassa on yhtenä vaatimuksena, että rikosepäilyissä organisaatio tekee rikosilmoituksen poliisille. Vaatimus on esitetty kaikille tietoturvatasoille suosituksena. Keskusrikospoliisin mukaan vaatimuksen tulisi olla ainakin korotetulla ja korkealla tietoturvatasolla vahvana suosituksena.

Keskusrikospoliisilla ei ole muuta yksityiskohtaisempaa lausuttavaa esitettyihin vaatimuskohtiin. Kohdat etenevät systemaattisesti tietoturvatasojen mukaisesti. Vaatimuskohdat ovat riittävän kattavia ottamalla huomioon, että kyseessä on ohjetasoinen ohjaava asiakirja. Keskusrikospoliisin näkemyksen mukaan ehdotetut vaatimukset soveltuvat hyvin käytettäväksi organisaatioiden tietoturvapoikkeamien käsittelyyn.

Keskusrikospoliisin päällikkö
Poliisineuvos
Robin Lardot

Turvallisuuspäällikkö, tietoturvavastaava
Rikoskomisario
Sami Rusanen