



24.1.2012

2020/2011/4757

Jakelussa mainitut

Valtiovarainministeriön lausuntopyyntö 2125/00.01.00.01/2011

POLIISIHALLITUKSEN LAUSUNTO TEKNISEN ICT-YMPÄRISTÖN TIETOTURVATASO-OHJEEN LUONNOKSESTA

Valtiovarainministeriö pyytää Poliisihallitukselta lausuntoa koskien Teknisen ICT-ympäristön tietoturvaso-ohjeen luonnosta.

Poliisihallitus toteaa että ohje on yleisellä tasolla tarpeellinen tarkentamaan muuttuneen regulaation ja ohjeiston vaatimuksia. Poliisihallituksen tietoturvapäällikkö Samuli Bergström on ollut mukana ohjeen valmistelussa ja tuonut poliisihallinnon kantaa esille jo valmistelutyön aikana.

Lisäksi Poliisihallitus toteaa muutamia yleisiä ja tarkentavia kommentteja ohjeluonnokseen.

Yleiset kommentit

Poliisihallitus pitää erityisesti ohjeen tekninen asiasisältö huomioiden perusteltuna, että ohjeen alussa on määritelty siinä käsitellyt keskeiset käsitteet sekä annettu lukuohje. Lisäksi ohjeessa on runsaasti asiaa selventävää kuvitusta, mikä helpottaa ohjeen omaksumista. Ohjeen hyvänä puoleena ovat myös sen liitteissä kuvatut konkreettiset apuvälineet ja työkalut. Ohjeessa on myös perustellusti käyty läpi kaikki ICT -palvelujen tuotantomallit ja todettu, että viime kädessä vastuu tietoturvallisuudesta on organisaatiolla itsellään palvelujen tuotantomallista riippumatta.

Toisaalta ohje pitää sisällään erittäin laajan aineiston, joten tulisi kiinnittää erityistä huomiota siihen, että vain ohjeen tarkoituksen kannalta keskeiset asiat käsitellään. Mikäli ohjetta halutaan yksinkertaistaa sen käytettävyyden lisäämiseksi, olisi myös mahdollista laatia yksinkertaistettu pääkohdat sisältävä versio ohjeesta.

Tulisi myös arvioida voitaisiinko ohjetta jakaa useampaan. Esimerkiksi tietojärjestelmän luokittelu ja järjestelmille asetettavat yleiset tekniset vaatimukset saattaisivat olla lukukelpoisemmat eri ohjeissa. Pääohjeessa on paljon yksityiskohtaisia teknisiä vaatimuksia jotka mahdollisesti voitaisiin siirtää eri tasojen teknisiksi vaatimuksiksi liitteisiin.

Yksityiskohtaiset kommentit

Ohjeluonnoksen sivun 12 kappaleessa 1.2 kuvataan kansainvälisen turvallisuusluokiteltavan tietoaineiston vaatimuksista suhteessa KATAKRlin. Oh-





jeen rajaukset tulisi tarkistaa voimassa olevan lainsäädännön mukaiseksi erityisesti kansallisen turvallisuusluokitellun tietoaineiston osalta.

Sivun 14 kappale 2.1 asetuksen vaatimusten konkretisointi on erittäin tarpeellinen ja hyvä osa ohjetta. Poliisihallitus ehdottaa kuitenkin seuraavaa tarkennusta kappaleeseen.

- Kohta 3 asiakirjojen käsittelyä koskevat tehtävät ja vastuiden määrittelyssä lieenee erittäin keskeistä, jopa luokitteluakin keskeisempää asiakirjahallinnon, diaarin ja tiedonohjaussuunnitelman määrittely.

Sivun 18 viimeisessä kappaleessa on käsitelty tietoaineistojen luokittelamista. Tässä yhteydessä tulisi nostaa korostetusti esille se, että vaatimus suojaustasoluokittelusta koskee kaikkia salassa pidettävää tietoaineistoa eikä vain turvallisuusluokiteltavaa aineistoa. Selvyyden vuoksi kappaleen loppuun asti jatkuvan kohdan, joka alkaa "Osaan salassa pidettävistä asiakirjoista voidaan tehdä..." voisi siirtää seuraavalle sivulle suojaustasoerittelyn jälkeen omaksi kappaleekseen.

Sivulla 20 oleva kuva viranomaisen asiakirjojen luokittelusta on havainnollinen ja siitä käy ilmi suojaustasomerkin ja turvallisuusluokitusmerkin erot. Tämänkin kuvan osalta olisi kuitenkin perusteltua korostaa sitä, että myös turvallisuusluokiteltu materiaali asetetaan jollekin suojaustasolle eli käytännössä myös turvallisuusluokiteltuun materiaaliin tulee suojaustasomerkinä (automaattisesti osana leimaa).

Sivulla 27 olevaan kuvaan nro 11 tulisi lisätä www -selain, koska se on käytännössä keskeinen tunkeutumisreitti ja osa viestintäpalveluita.

Ohjeluonnoksen sivulla 29 on kuvattu kahden erillisen teknisen ympäristön rakentaminen. Mainittu ratkaisu vaatii usein merkittäviä rahallisia lisäresursseja, joten käytännössä sen toteuttaminen ei läheskään aina tiukan taloudellisen tilanteen vuoksi ole mahdollista, vaikka tietoturvallisuuteen liittyvät seikat tätä edellyttäisivät. Lisäksi kuvaa olisi perusteltua tarkentaa siten, että samalla työasemalla ei voida liikkua molemmissa ympäristöissä ilman, että erotetaan ympäristöt työasemassa esimerkiksi eri käyttäjätunnuksilla.

Sivulla 35 kohdassa "Esimerkkejä tietoliikenneyhteyteen liittyvistä teknisistä ratkaisuista..." on mainittu "tarvittava lokitus ja hälytysten tuottaminen sekä niihin reagoiminen". Tässä yhteydessä olisi tärkeää ilmaista, että lokiin tulee kirjata nimenomaan onnistuneet yhteydet eikä ainoastaan palomuurin estämiä yhteyksiä. Tietoturvapoikkeamat syntyvät erityisesti onnistuneista tunkeutumisista, joten juuri niiden tulee kirjautua lokiin.

Sivun 36 kohtaan "Esimerkkejä palvelinympäristöön liittyvistä teknisistä ratkaisuista..." olisi perusteltua lisätä kaksi kohtaa:

- viranomaisen tiedon suojaaminen pääkäyttäjäoikeuksin toimivilta (ulkoistetuilta) ylläpitäjiltä silloin, kun se on käytännössä mahdollista esimerkiksi tietokannan sisällön salakirjoittamisella
- lokitiedon siirtäminen automaattisesti palvelimen ulkopuolelle keskitettyyn ja suojattuun lokipalvelimeen



Sivulle 51 kohtaan "3. Dedikoitu ympäristö - toimittajan ylläpitämä ympäristö - palvelu tuotetaan Suomesta" tulisi huomioitavien seikkojen listaan lisätä seuraavat kohdat:

- ulkoistava organisaatio saattaa menettää oikeuden käsitellä lokitietoa tietoturvapoikkeaman selvittämiseksi. Ellei muuta sovita, palveluntarjoaja saattaa myös laskuttaa lokitiedon käsittelystä asiantuntijapalkkion
- uuden pakkokeinolain voimaantullessa ei ulkoistavalla organisaatiolla, ulkoistetun palvelun tarjoajalla eikä esitutkintaviranomaisella ole lähtökohtaisesti oikeutta selvittää lokitiedoista ulkoistetun palveluntarjoajan työntekijän tekemää salassa pidettävän viranomaistiedon päätymistä oikeudettomasti ulkopuolisille

Sivulle 52 huomioitaviin seikkoihin tulisi lisätä maininta siitä, että henkilötietoja ei saa siirtää ETA -alueen ulkopuolelle prosessia tarkastamatta ja ettei suomalaisten viranomaisten toimivalta ulotu Suomen rajojen ulkopuolelle.

Ohjeen sivulla 64 oleviin vaatimuksiin tulisi lisätä lokien käsittelyoikeuden toteuttaminen siten, ettei palveluntarjoajalla ole oikeutta pyytää palkkiota jokaisesta lokitietoihin liittyvästä käsittelytoimenpiteestä.

Poliisijohtaja



Sauli Kuha

Tietoturvapäälikkö



Samuli Bergström

Jakelu

Valtiovarainministeriö

Tiedoksi

Sisäasiainministeriö poliisiosasto