3.6.2010

Poha Dno/2010/1948

Valtiovarainministeriö

VM kirje 19.5.2010

POLIISIHALLITUKSEN LAUSUNTO KOSKIEN LUONNOSTA VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMAKSI

Asia

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on pyytänyt Poliisihallitukselta lausuntoa valtionhallinnon tietoturvallisuuden kehitysohjelmasta. Lausunto kattaa myös muiden lausuntopyynnössä mainittujen poliisin yksiköiden kommentteja.

Lausuntopyynnön mukaan lausunnossa tulee käsitellä seuraavat asiat:

1) hallinnonalan tai viraston kannanotot ja ehdotukset kehitysohjelman sisältöön, toimenpiteisiin, painotuksiin ja toimeenpanoon
2) hallinnonalan tai viraston nykyiset edellytykset ja valmiudet kehittämisohjelman toimeenpanoon ja yhteistyöhön
3) kehitysohjelman hyödyt hallinnonalan tai viraston kannalta
4) kehitysohjelman toimeenpanon edellyttämät toimenpiteet sekä resurssi- ja kustannusvaikutukset hallinnonalalla tai virastossa
5) hallinnonalan tai viraston ilmoitukset organisaation omista osallistumisista hankkeisiin ja kehityskohdetason valtiotasoisen yhteistyön toteuttamiseen sekä kohdekohtaiset yhteyshenkilöt

Kommentit

Poliisihallitus toteaa kunnioittavasti että Valtiovarainministeriön luonnosvaiheessa oleva kehitysohjelma on kattava ja pääpiireiltään vastaa myös poliisin näkemystä tietoturvallisuuden kansalliseksi kehityssuunnaksi. Yksittäiset kommentit on järjestetty asiakohdittain.

Hallinnonalan tai viraston kannanotot ja ehdotukset kehitysohjelman sisältöön, toimenpiteisiin, painotuksiin ja toimeenpanoon

Luonnoksen keskeinen sisältö on voimakas konserniohjauksen vahvistaminen. Ohjauksen lisääntyminen on kansallista tietoturvatasoa kokonaisuutena lisäävä tekijä ja siten positiivinen suuntaus. Lisääntyvässä ohjauksessa on syytä kuitenkin huomioida valtionhallinnon toimijoiden erityistarpeet sekä jo tehdyt linjaukset tai panostukset tietoturvallisuuteen. Tietoturvallisuutta ei tarvitse tai kannata hallita kaikissa virastoissa samalla tavalla kunhan lopputulos voidaan arvioida yhteisillä kriteereillä.

Tietoturvallisuuden kansallisten kriteerien ja arvioinnin edelleen täsmentyminen vertailukelpoisemmaksi on positiivinen asia ja kehittää luottamusta viranomaisten kesken. Tämä osaltaan parantaa valmiuksia myös tiivistyvään viranomaisyhteistyöhön ja tietojenvaihtoon. Samalla yhdenmukaisen toiminnan kautta myös kansalaisen luottamus viranomaisen tietoturvallisuuden hallintaan paranee. Kriteerien ja vaatimusten laadinnassa sekä arviointityössä tulisi kuitenkin selvästi huomioida että valtionhallinnossa tulee jatkossakin olemaan eri kypsyystasoilla toimivia virastoja. Siten eri tasoilla olevien palveluiden, virastojen tai muiden yhteistyökumppanien välille onkin tärkeä luoda yhteiset kontrollit ja mittarit joilla yhteistyö voidaan toteuttaa turvallisesti.

Tietoturvallisuuden kehittämiseen suunnatut resurssit tulevat tehokkaimmin käytetyksi siten, että tietoturvallisuutta kehitetään erityisesti siellä, missä sen taso ja laatu on vaarassa jäädä keskimääräistä alhaisemmalle tasolle. Valtionvarainministeriöön keskitetty koko valtionhallintoa koskeva tietoturvallisuuden kehittäminen on omiaan kohdentamaan toimenpiteitä niihin hallinnonaloihin ja virastoihin, joiden tietoturvallisuustason voidaan katsoa olevan keskimääräistä alhaisempi. Toisaalta kehittämisohjelmaa toteutettaessa tulee huomioida se, että myös tiettyjen hallinnonalojen ja virastojen erityistarpeet tulevat huomioiduiksi ja että tietoturvallisuuden kehittäminen jatkuu aktiivisena ja tehokkaana myös siellä, missä se tällä hetkellä on suhteellisen korkealla tasolla.

Poliisihallitus pitää perusteltuna sitä kehitysohjelmaluonnoksessa esitettyä kantaa, että virastoille asetetaan osana tulosohjausta konsernitason tietoturvatavoitteita sen sijaan, että tietoturvaosaajat keskitettäisiin konsernin tarpeisiin. Koska tietoturvatavoitteiden saavuttaminen edellyttää sekä henkilöllisiä että taloudellisia resursseja, virastoille tulisi luonnollisesti antaa tarvittavat resurssit tulostavoitteisiin pääsemisen varmistamiseksi.

Kehitysohjelman keskeisenä tavoitteena on se, että tietoturvallisuutta koskevat näkökohdat saadaan integroiduksi hallinnon johtamiseen, kehittämiseen, palveluihin, prosesseihin ja ict-toimintaan (kokonaisvaltaisuus ja läpäisy). Organisaatioiden tulee muun ohella kehittää palvelu- ja hankintaketjujen tietoturvallisuuden hallintaa. Merkittäväksi tekijäksi tietoturvallisuuden kehittämisessä ovat nousseet erilaisten tietojärjestelmien tietoturvallisuusnäkökohdat. Keskeinen osa tietojärjestelmän tietoturvallisuuteen vaikuttavasta työstä tehdään jo järjestelmän hankintavaiheessa (viitattu myös kehitysohjelman kohdassa 5.3.1). Tietoturvallisuusnäkökohtien huomioiminen jo hankittavan järjestelmän suunnittelutyössä ja vaatimusmäärittelyissä tukee tietoturvatavoitteiden saavuttamista ja on myös taloudellisesti tehokasta, koska tietoturvallisuuteen liittyvien muutosten tekeminen valmiiseen järjestelmään on monimutkaista ja kallista. Viime kädessä konsernitasolla tulisi varmistaa, että tietoturvanäkökohdat tulevat huomioiduiksi erityisesti juuri järjestelmähankinnoissa ja tähän tarkoitukseen tulisi olla keskitetysti saatavissa yhdistettyä ict-, hankinta- ja tietoturvallisuusosaamista.

Keskeistä tietoturvallisuuden ohjauksen kehittymiselle on tietoturvallisuusasetuksen voimaantulo erityisesti tietoturvatasojen kautta. Valitettavan kuvaavaa on että asetuksen voimaantulon päivämäärä on edelleen avoinna myös luonnoksessa (sivu 14). Tietoturvallisuusasetuksella on suuri periaatteellinen merkitys tietoturvallisuuden kehittämisen kannalta, koska asetus koskee yhteisesti kaikkia hallinnonaloja ja monet vielä nykyään esimerkiksi sisäasiainministeriön antamiin määräyksiin sisältyvät velvoitteet (esim. tiedon luokitteleminen ja käsittelyvaatimukset) nostetaan asetuksen tasolle. Asetuksen siirtymäsäännökset siirtymäaikoineen katsotaan perustelluiksi.

Kehitysohjelman sivulla 16 (kohdan 4.1.1 toinen kappale) on todettu muun muassa, että ”IT-organisaatio toteuttaa järjestelmien ja palvelujen omistajien tietoturvavaatimukset.” Asiassa tulisi huomioida se, että IT-organisaation tehtävänä on nimenomaan teknisten tietoturvavaatimusten toteuttaminen. IT-organisaatiota ei kuitenkaan tulisi katsoa kaikkien tieto-

turvavaatimusten toteuttajaksi, vaan nimenomaan teknisten tietoturvavaatimusten toteuttajaksi. Tämä seikka tulisi huomioida kehitysohjelmassa.

Luonnoksen sivulla 19 (kohdan 4.1.2.1 ensimmäinen kappale) on otettu esille tietoturvallisuuden tekninen puoli toteamuksella "Johtajien ymmärtämys teknologiavaikutuksista ja käyttöönoton seurauksista on tärkeää, jotta he voivat tehdä toimintaa ja teknologiaratkaisuja koskevia päätöksiä. Teknologian ja tietojärjestelmien tietoturvavaikutukset tulee ymmärtää tarkemmin johtamiseen liittyvässä tulosohjauksessa." Tässäkin yhteydessä tulisi huomioida se, että tekninen tietoturvallisuus on vain yksi tietoturvallisuuden osa-alueista, joten olisi perusteltua arvioida asiaa myös muiden tietoturvallisuuden osa-alueiden, kuten hallinnollisen tietoturvallisuuden, näkökulmasta. Johtajien tulee toisin sanoen ymmärtää se, että tietoturvallisuus on paljon muutakin kuin vain teknistä turvallisuutta.

Poliisihallitus pitää perusteltuna kehitysohjelman ehdotusta siitä, että tietoturvallisuuden kehittämistä ja toteuttamista tultaisiin ohjaamaan konsernimaisesti valtionhallinnossa ja että tähän ohjaustehtävään lisätään tarvittaviksi katsotut henkilöresurssit. Resurssien keskittäminen konserniohjaukseen tulisi kuitenkin toteuttaa siten, ettei keskittäminen johtaisi esimerkiksi virastojen resurssien vähentämiseen samassa suhteessa. Vaikka keskitetty ohjausmalli tulee toteutuessaan vähentämään joitakin tietoturvallisuuteen liittyviä tehtäviä, tulee erilaisten virastotason tehtävien määrä todennäköisesti kasvamaan samassa yhteydessä. Seikka on ollut esillä myös kehitysohjelmassa (kohta 4.2.2), jossa on lausuttu, että virastot tulevat jatkossakin tarvitsemaan omia tietoturvaresursseja perusasioiden toiminnan varmistamiseen, toiminnan koordinoimiseen sekä ostamisen asiantuntijatehtäviin.

Kehitysohjelmassa on hahmoteltu myös tietoturvallisuuden mittaamiseen ja raportointiin liittyviä toimenpiteitä. Yhteinen valtionhallinnon tietoturvaraportointiväline mahdollistaa pohjaltaan yhteismitallisen sekä kohtalaisen ajantasaisen kuvan saamisen tietoturvallisuuden tilasta ja siihen liittyvistä ilmiöistä valtionhallinnossa. Poliisin näkökulmasta on toivottavaa, että tehdyn raportoinnin perusteella saadaan palautetta ja että raportoinnin vaikutuksista konsernitason päätöksentekoon ja toimenpiteisiin myös informoidaan aktiivisesti virastotasoa. Raportoinnin toivotaan huomioivan myös organisaation nykyiset välineet jotta vältytään monenkertaiselta raportoinnilta.

Globaali toimintaympäristö asettaa enenevissä määrin myös valtionhallinnolle vaatimuksia kansainväliseen yhteistyöhön. Valtionhallinnon arviointikriteerien parempi ulottaminen vastaamaan kansallisten toimijoiden lisäksi myös kansainvälisiä kumppaneita toisi pohjan yhteisen kontrollirakenteen syntymiselle.

Poliisi pitää perusteltuna vakituisen tietoturvallisuuden tarkastusjaoston perustamista. Pelkästään tietoturvallisuuteen ja tiedon turvaamiseen keskittyvällä pysyvällä elimellä voidaan katsoa olevan realistiset mahdollisuudet ottaa kattavasti haltuun tietoturvallisuutta koskeva laaja toimintakenttä.

Kehitysohjelman tietoturvaosaamista ja koulutusta koskevat kannanotot ovat poliisin näkemyksen mukaan hyvin keskeisiä tietoturvallisten toimintatapojen käytännön toteutumisen kannalta. Työntekijöiden tietoturvallisuus-

osaamisen sisällöllisen kehittämisen ohella huomiota pitää kiinnittää erityisesti asenteisiin ja työpaikoilla vallitseviin toimintakulttuureihin.

Turvallisen sähköisen hallinnon yhteydessä kehitysohjelmassa on tarkasteltu muun ohella tiedon omistajuutta ja siihen liittyvien vastuiden selkiyttämistä (kohta 5.2.1.2). Useat kyseisessä kohdassa mainitut toimenpiteet ovat perusteltuja. Toimenpiteiden toteuttaminen käytännössä edellyttää virastoilta myös huomattavaa työpanosta. On huomattava, että toimenpiteiden tuloksena tulisivat olemaan muun muassa koko valtiokonsernin kattavat yhdenmukaiset tietojen luokitukset ja niiden mukaiset käsittely- ja suojausmenettelyt, joten kyseessä on käytännön ohella periaatteellisestikin suuri kehitysaskel.

Viraston nykyiset edellytykset ja valmiudet kehittämisohjelman toimeenpanoon ja yhteistyöhön

Poliisi on viime vuosina aktiivisesti kehittänyt tietoturvallisuutta. Tietoturvallisuuden kehittäminen on perustunut muun muassa Valtion tietoturvallisuuden johtoryhmän (VAHTI) ohjeistuksiin sekä poliisin omiin tietoturvaperiaatteisiin. Poliisiin on muun muassa muodostettu hallinnon sisäinen turvallisuusorganisaatio ja käytössä on esimerkiksi säännöllinen tietoturvaraportointi, sähköinen tietoturvallisuuskoulutus sekä sähköinen käyttövaltuuksien hallinnointi (tunnushallinta). Lisäksi muun muassa tietoaineiston luokittelemisesta ja käsittelystä on annettu määräysten tasoista normistoa. Voidaankin arvioida, että tietoturvallisuuden kehittäminen ja hallinnointi on keskimäärin hyvällä tasolla.

Poliisi on pyrkinyt toiminnassaan ottamaan mahdollisimman laajasti huomioon hallinnonalaa koskevat tietoturvallisuuslinjaukset, -politiikat ja -periaatteet ja niiden mukaiset toimintamallit. Tämän tuloksena virastoon on jo tähän mennessä muodostunut tietoturvallisuuteen liittyviä vakiintuneita käytänteitä ja tietoturvallisuuden toteuttamiseen liittyvät tehtävät on sisällytetty organisaation toimintaan. Edellä kerrotun perusteella poliisi katsoo, että sillä on hyvät edellytykset ja valmiudet tietoturvallisuuden edelleen kehittämiseen ja kehittämisohjelman toimeenpanoon sekä yhteistyöhön. Kehittämisohjelman asianmukainen toimeenpano edellyttää kuitenkin sitä, että siihen varataan riittävät henkilöstöresurssit.

Kehitysohjelman hyödyt

Keskeisenä tietoturvallisuuden kehitysohjelman hyötynä voidaan nähdä koko valtiokonsernin keskitetty tietoturvallisuustason nousu. Tärkeää on erityisesti tietoturvallisuustason nostaminen niillä sektoreilla, joilla taso on keskimääräistä alhaisempi. Lisäksi tietoturvallisten toimintamallien, tietoturvallisuuden käsitteiden sekä kulttuurien yhdenmukaistuminen parantaa edellytyksiä eri toimijoiden väliseen yhteistyöhön sekä parantaa osaltaan kansalaisten luottamusta valtionhallinnon organisaatioiden toimintaan.

Kehitysohjelman erityiseksi hyödyksi voidaan myös nähdä se, että tietoturvallisuuden kehittämiseen tullaan omaksumaan pitkäjänteinen asenne sekä aiempaa laajempi näkökulma. Kehitysohjelma ohjaa uuden kehittämisen

ohella suuntaamaan huomiota myös siihen, ovatko jo olemassa olevat tietoturvallisuuskäytännöt ja -normit ajantasaisia ja tehokkaita virastossa.

Eräs välttämätön tekijä tietoturvallisuuden kehittämisen kannalta on se, että tietoturvallisuuden tasoa kyetään mittaamaan luotettavasti (kehitysohjelman sivu 20, kohta 4.1.2.2). Vasta täsmälliset tiedot kehittämisen kohteesta mahdollistavat tehokkaat kehittämistoimenpiteet. Yhtenäisillä ja luotettavilla tietoturvallisuuden mittareilla saadaan tietoa siitä, miten toiminta kehittyy ja mikä on kehityksen suunta ja nopeus.

Kehitysohjelman toimeenpanon edellyttämät toimenpiteet sekä resurssi- ja kustannusvaikutukset

Kehitysohjelman toimeenpanon edellyttämiä toimenpiteitä ja sen vaatimia resursseja on tässä vaiheessa hankalaa arvioida yksityiskohtaisesti. Koska kehitysohjelman tavoitteena on integroida tietoturvallisuus voimakkaammin lähes kaikkeen viraston toimintaan, ohjelman ja sen toteuttamisen vaikutukset hajautuvat siten, että kokonaisarvioinnin tekeminen on vaikeaa. On selvää, että tietoturvallisuutta koskevien näkökohtien lisääntyvä huomioiminen toiminnassa lisää myös tarvetta tietoturva-asiantuntijoiden käyttämiseen. Eräänä keskeisenä tavoitteena oleva henkilöstön tietoturvaosaamisen parantaminen ja koulutus tulee myös vaatimaan ajallisia resursseja sekä koulutettavalta henkilöstöltä että koulutuksen koordinointiin ja toteuttamiseen osallistuvilta.

Tietoturvavaatimusten painotettu huomioonottaminen esimerkiksi järjestelmähankinnoissa tulee väistämättä johtamaan kasvaviin hankintakustannuksiin, mutta kehitysohjelmassakin linjatulla tavalla tavoitteena tulee olla se, että tietojen käytettävyys, luottamuksellisuus ja eheys varmistetaan.

Ilmoitukset organisaation omista osallistumisista hankkeisiin ja kehityskohdetason valtiotasoisen yhteistyön toteuttamiseen sekä kohdekohtaiset yhteyshenkilöt

Poliisihallituksen tietoturvallisuuden yhteyshenkilönä toimii poliisin tietoturvapäällikkö Samuli Bergström. Poliisin osallistuminen hankkeisiin arvioidaan tapauskohtaisesti.

Poliisijohtaja Sauli Kuha

Tietoturvapäällikkö Samuli Bergström