Mavi

MAASEUTUVIRASTON LAUSUNTO VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMASTA (VM047:00/2007)

Maaseutuvirasto pitää tärkeänä tietoturvallisuuden hallittua kokonaisvaltaista kehittämistä. Ohjelmassa ehdotettu konserniohjauksen vahvistaminen on kannatettavaa ja oikein mitoitettuna sekä toteutettuna sillä voidaan saavuttaa hyviä tuloksia. Maaseutuviraston mielestä kuitenkin kokonaistavoitetilanne pitäisi huomioida selkeämmin kattaen konserni-, hallinnonala- ja virastotason. Vaarana on muutoin erittäin raskaat menettelyt sekä virheelliset vastuujaot tai niiden olettamat. Ohjelmaluonnoksen mukainen resurssien määrän lisääminen Vm:n konserniohjaukseen ja hallinnonalojen oman työpanoksen vähentäminen tuo myös riskin toiminnan tietoturvaosaamisen siirtymisestä kauemmas toiminnasta ja virastokohtaisten erityispiirteiden jäämisestä huomiotta. Ohjelmaluonnoksessa ehdotetaan myös konsernitason tietoturvallisuuden osaamisvajeen paikkaamisesta esimerkiksi siirtämällä perustoiminnoista ja -prosesseista henkilöitä konsernitasolle koulutuksen kautta tekemään tietoturvatehtäviä joko tilapäisesti tai pysyvästi. Kuitenkin ottaen huomioon virastojen substanssitoimintojen ja tuottavuusohjelman haasteet, tämän tyyppinen henkilöstön siirto konsernitasolle on hyvin haasteellinen toteuttaa ilman että virastojen substanssitoiminta kärsii. Ohjelmaluonnoksessa ehdotetaan myös henkilöstön uudelleen- ja täydennyskoulutusta tietoturva-asiantuntijoiksi, mikä on hyvä lähtökohta. Lopputulos tulee kuitenkin olla IT- ja substanssiasiantuntijoiden tietoturvaosaamisen vahvistaminen ja hyödyntäminen omassa työssä ei resurssin siirto pelkästään tietoturva-asiantuntijan tehtäviin.

Ohjelmaluonnos myös edellyttää virastoilta riittävien resurssien varaamista tietoturvatoimintaan. Nykyisen valtionhallinnon tuottavuusohjelman mukaisten henkilöstön vähentämisohjelman puitteissa virastoilla ei kuitenkaan ole välttämättä henkilökehyksen puitteissa mahdollisuutta taata ohjelmaluonnoksen edellyttämää riittävää resurssia tietoturvatoimintaan ellei tarvetta oteta huomioon henkilökehyksen mitoituksessa. Tietoturvan tuominen tulosohjaukseen antaa tähän kuitenkin työkaluja. Riskienhallinnan merkitystä tulisi korostaa enemmän myös resurssien hallinnassa ja kohdentamisessa. Muutoin on vaarana kokonaisuuden hämärtyminen ja resurssien tuhlaus - Riskien arviointiin ei satsata riittävästi, koska kontrollit on joka tapauksessa toteutettava, oli niihin varaa tai ei. Tietoturvallisuuden johtamisen ja hallinnan kansainvälinen standardi (ISO 27001) painottaa ottamaan huomioon toiminnan luonteen ja tarpeet sekä etsimään menettelyjä, jotka hyödyttävät organisaatiota.

Tiedon elinkaariajattelun painotus tarkoittaa käytännössä tietoturvallisuuden tarkastelemista nykyistä tiiviimmässä yhteydessä kaikkeen tiedonhallinnan suunnitteluun. Siksi olennaista kehitysohjelman onnistumisessa on, että tiedon kaikki hallintatavoitteet ja -toimet ovat tasapainoisesti mukana kehittämisessä ja että osakokonaisuuksien hyvän hallinnan lisäksi konsernissa ja organisaatiossa hallitaan myös tietojen hallinnan kokonaisuutta. Osaalueiden tuominen nykyistä tiiviimpään yhteyteen mahdollistaisi synergiahyötyjen saavuttamisen toiminnan ja sen tietoturvallisuuden kehittämisessä.

Järjestelmäturvallisuuden ja toiminnan turvallisuuden rajaa on pyrittävä nykyisestä häivyttämään, koska tietojen sähköinen hallinta ja säilyttäminen muuttaa myös toiminnan turval-

lisuuden hallinnan järjestelmäpainotteiseksi. Organisaation sähköinen asian- ja tiedonhallinta kiinnittyy aiempaa voimakkaammin erilaisiin toiminnan hallintaprosesseihin (kuten palveluiden ja tietojen ohjaus), jotka edellyttävät taustalle monimutkaisia IT-hallintarutiineja. Toisaalta sähköiset asiointipalvelut kiinnittävät asian- ja tiedonhallinnan sekä taustalla olevan IT:n entistä voimakkaammin myös toiminnan prosesseihin. Järjestelmäturvallisuuden hyvän hallinnan lisäksi tietoturvaosaamista onkin kehitettävä ja kohdennettava siten, että se yhdistyy nykyistä kokonaisvaltaisemmin toimintojen ja prosessien ja niissä syntyvien tietoaineistojen turvallisuuden parantamiseen.

Tiedon säilyttämiseen kohdistuu myös muita kuin tässä kehitysohjelmassa mainittuja vaatimuksia. Esimerkiksi tiedon suojaamista koskevia luokitteluita ja periaatteita olisi syytä yhteismitallistaa, mikä edellyttää tiivistä yhteistyötä tietoturvallisuuden ja asiakirjallisen tiedon säilyttämisen kehittämisestä vastaavien viranomaisten kesken. Arkistolaitoksen Sähke2-määritys edellyttää tietojen sähköiseltä säilyttämiseltä tietoa kuvailevia metatietoelementtejä ja niihin pohjautuvia it-toiminnallisuuksia, joilla sähköisesti säilytettävien tietojen kiistämättömyys ja muuttumattomuus voidaan taata. Ne asettavat tietoturvallisuuden kehittämiselle keskeisiä vaatimuksia, joiden asema suhteessa tämän kehitysohjelman tavoitteisiin ja tietoturvallisuuden hyvän hallinnan kokonaisuuteen on määriteltävä selkeästi.

Tietoturvallisuuden hyvä hallinta edellyttää siten nykyistä laajempaa tarkastelua ja osaamisen kehittämistä IT-turvallisuuden, asiakirjatietoturvallisuuden ja prosessien toiminnan turvallisuuden kesken. Organisaatioissa tiedonhallintaan keskittyvät resurssit ovat yleensä varsin niukkoja ja keskittämättömiä. Kehitysohjelman tehokkuuden ja onnistumisen kannalta on tärkeää, että tietoturvallisuuden osa-alueiden hallinta kyetään kursimaan hallittavaksi kokonaisuudeksi myös toiminnan perusteissa ja ylätason ohjauksessa.

Ylijohtaja Leena Tenhola

Osastonjohtaja Mika Tuikkanen