Poliisihallitus

Lausunto

02.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Poliisihallituksen lausunto; Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta 2024-2035

Poliisihallitus kiittää Liikenne- ja viestintäministeriötä mahdollisuudesta lausua Valtioneuvoston periaatepäätökseen Suomen kyberturvallisuusstrategiasta 2024-2035. Poliisihallitus on osallistunut kyberturvallisuusstrategian valmisteluun osana Sisäministeriön valmistelutyötä kevään 2024 aikana. Poliisin näkökulmia on tuotu lausunnon kohteeseen jo valmistelun aikana.

Poliisihallituksen lausunto keskittyy niin poliisille kuuluvien lakisääteisten tehtävien kuin viraston kyberturvallisuuden varmistamiseen. Yhteiskunnan turvallisuusstrategian perusperiaatteiden mukaisesti toimivaltaiset viranomaiset vastaavat häiriötilanteiden hallinnasta ja siihen liittyvästä varautumisesta. Poliisi vastaa osaltaan viraston kyberturvallisuudesta. Poliisilla on tämän lisäksi omassa roolissaan kyberturvallisuuden ylläpitämiseen ja kyberrikostorjuntaan liittyviä lakisääteisiä poliisitoiminnallisia tehtäviä.

Poliisi osallistuu muiden valtion virastojen ja toimijoiden tavoin kansallisen kyberturvallisuuden ylläpitämistä. Poliisista osallistuu työhön niin kyberrikostorjunnan kuin kyberturvallisuuden asiantuntijoita. Strategiakirjausten osalta pyydetään huomioimaan poliisin eri tehtävät lakisääteisten poliisitoiminnallisten tehtävien kuin poliisin oman organisaation suojaamisen osalta sekä tarvittaessa erottamaan nämä kaksi roolia toisistaan. Kyberturvallisuuden toteuttaminen toimintaympäristön muuttuneissa olosuhteissa ja erittäin nopeasti kehittyvien uusien teknologioiden tuomien uhkien parissa edellyttää selkeää resurssointia organisaatiolle. Tämä näkökulma on todettu strategiassa. Sen keskeisyyttä ja merkitystä mm. valtionhallinnon organisaatioille voisi olla hyvä korostaa edelleen. Myös riittävä resurssointi ja tuki tarvitaan valtion yhteisiä palveluita tarjoaville toimijoille kuten Valtorille ja Suomen Erillisverkoille.

Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035 asti. Aikaisempia kyberturvallisuusstrategioita pidemmällä strategiakaudella mahdollistetaan strategian mukaisten toimenpiteiden tosiasiallinen suunnittelu ja toteuttaminen sekä toimenpiteiden edellyttämien resurssien esittäminen ja varmistaminen. Strategiakauden aikana laadittavilla toimenpideohjelmilla tai vastaavilla strategiasta johdettujen asiakirjojen kirjausten toimenpiteillä on näin ollen mahdollista saavuttaa strategiassa määritellyt tavoitteet.

Kehityssuunta strategiakauden pidentämisessä on hyvä, sillä aiempien kyberturvallisuusstrategioiden osalta valtion budjetointi- ja rekrytointiprosessit eivät mahdollistaneet toivotulla tavalla pitkäjänteistä kyberturvallisuuden

kehittämistä virastoissa. Pitkäjänteisyys on keskeinen tekijä, koska virastojen palvelutuotannon mallien, ict-infrastruktuurin ja tietojärjestelmien osalta tehdyt valinnat ja päätökset eivät rajoitu strategiakauteen. Pitkäjänteisyys korostuu poliisin osalta myös poliisille palveluita tuottavien keskeisten valtionhallinnon perustietotekniikkapalveluiden tuottajien ja erityisesti turvallisuusverkon Tuve-palvelutuottajien kehittämisen malleissa.

Kyberturvallisuuden ja laajemmin valtionhallinnon toiminnan kehittämisessä korostuu erilaisten kehittämishankkeiden keskinäinen koordinointi sekä tavoitteiden asettaminen. Valtionhallinnon säästötoimenpiteet virastoille aiheuttavat haasteita niin uusien käyttöönotettavien teknologioiden kyberturvallisuuden varmistamisen osalta kuin käytössä olevan vanhentuneen ict:n kyberturvallisuusvaatimusten osalta. Kyberturvallisuustyön yhdistäminen muuhun käynnissä olevaan strategia tason työhön sekä käytössä olevaan rahoitukseen nähdään poliisissa tärkeänä. Virastoille osoitetut vaatimukset edellyttävät vaatimusten mukaista rahoituksen ja resurssien järjestämistä. Valtiontaloutta tasapainotettaessa tulee huomioida kyberturvallisuuden varmistamisen ja sen aikana syntyvien uusien innovaatioiden tuottamat säästöt ja potentiaali.

Pidemmällä aikavälillä tapahtuneen analogisesta tietoaineistosta digitaalisten tietoaineistojen tietojenkäsittelyyn siirtymisen myötä kyberturvallisuuden varmistamisen luonne on muuttunut. Taustalla tapahtuva muutos tarkoittaa perinteisten turvallisuustyön roolien uudelleen arviointia. Kyberturvallisuus on osa kokonaisturvallisuutta. Kyberturvallisuuden johtaminen vaatii avointa ja uudenlaista näkemystä siitä, miten kykenemme jatkossa varmistamaan toiminnallisten prosessien turvallisuuden.

Uusien ja nousevien murrosteknologioiden kehityskulkua on haastavaa arvioida ennalta. Kyseiset teknologiat ja näiden taustalla vaikuttavat valinnat edellyttävät myös kyberturvallisuuden varmistamisessa uusia keinoja ja resursointia. Virastojen siirtyminen paikallisesti tuotetuista ict-ratkaisuista palveluntuottajien pilvipalveluihin tai palveluntuottajien pilvipalvelujen kaltaisista palvelutuotannon malleista tuottamiin palveluihin edellyttää kyseisten teknologioiden kyberturvallisuuden osaamisen ja kyberturvallisuuden vaatimusten kehittämistä.

Yksittäisen viraston näkökulmasta kyberturvallisuuteen tai sen lähelle kuuluvien vaatimusten sirpaloituminen haastaa virastojen kyberturvallisuustyön jatkuvasti. Yksi luonteva kyberturvallisuusstrategian strategiakauden tehtävistä onkin arvioida miten virastot voivat riittävällä tavalla varmistua, että vaatimukset on täytetty. Osana tätä julkisten palveluiden arviointikriteeristöä on selkiytettävä. Strategiassa tulisi nostaa yhdeksi tärkeäksi toteutukseksi yhteisen kriteeristön tuottaminen valtion hallinnon organisaatioille sekä sen yhtenäinen käyttäminen. Kriteeristö voisi olla myös muun yhteiskunnan hyödynnettävissä.

Uusien ja nousevien murrosteknologioiden myötä myös turvallisuustyön tekijöiden muuttuvaa profiilia tulee arvioida sekä strategioiden kautta ohjata mikä on se osuus kyberturvallisuustyöstä, johon virastojen tulee tulevaisuudessakin kyetä vastaamaan. Kyseessä on rajanvetoa siitä mitä virastot voivat ulkoistaa esimerkiksi muille kuin valtionhallinnon keskitetyille palveluntuottajille ja mikä on valtionhallinnon näkökulmasta sellaista kriittistä osaamista, jota ei voi ulkoistaa. Nyt asia on pitkälti yksittäisen viraston harkittavissa. Kokonaisohjaus tässä tuottaisi yhdenmukaisuutta sekä näin parantaisi kokonaisturvallisuutta.

Keskeisimpien kaikkia valtionhallinnon toimijoita koskevien muutosten yh teydessä tulisi yhä vahvemmin arvioida kyberturvallisuuden varmistamista yhteiskunnan kokonaisturvallisuuden näkökulmasta. Valtion perustietotekniikkapalveluita tuottavien toimijoiden tuottamien palveluiden lisäksi virastot tuottavat myös itse sellaisia palveluita ja toiminnallisia kokonaisuuksia, joiden tuottamisessa tulee huomioida kyberturvallisuuden varmistaminen kokonaisuudessaan ja yhtä virastoa laajemmasta näkökulmasta. Esimerkiksi tekoälyteknologioiden käyttöönottojen yhteydessä tilannetta arvioidaan

usein yhden yksittäisten viraston hyötyjen näkökulmasta, jolloin esimerkiksi taustalla olevien keskitettyjen alustaratkaisujen ja kyseisen tekoälyteknologian yhteisvaikutuksia ei arvioida koko käyttäjäkunnan näkökulmasta. Toisaalta hyödyt jäävät yksittäiselle virastolle.

Uusien teknologioiden osalta esimerkiksi kvanttiteknologian hyödyntämisessä ja etenkin salausteknologioiden kehittämisessä valtion tulisi yhä vahvemmin tukea kehitystyötä. Tämän tulisi olla strategisen tason asia, jotta voimme kansallisesti varautua tulevaisuuden muutoksiin sekä mahdollisesti luoda uutta kilpailukykyä suomalaisille yrityksille.

Kyberturvallisuuden tilannekuvaan liittyvä kehitystyö on ollut yksi aiempien kyberturvallisuusstrategioiden keskeisiä elementtejä. Tulevalla strategiakaudella tilannekuvat ja niihin liittyvät työkalut edellyttävät konkreettisia toimenpiteitä. Valtion yhteisten palveluntuottajien ja asiakkaiden yhteiset työkalut ja näkymät ovat tässä ensiarvoisen tärkeitä. Tätä on mahdollista ohjata strategiaan tehtävillä kirjauksilla, jotka myöhemmin viedään toimenpiteinä toimenpideohjelmiin. Strategiassa painotetaan tärkeyttä oman ict-ym päristön tuntemukselle. Tuntemus edellyttää riittäviä tietoja palveluntuottajilta. Kyberturvallisuuden näkökulmasta strategiassa tulee painottaa virastoille palveluja tuottavien palvelutuottajien roolia kaiken oleellisen kybertilannekuvaan ja asiakkaiden ympäristöihin liittyvän tiedon jakajana.

Tiedonkulussa ja tilannekuvien tuottamisessa korostuu poliisin osalta aiemmin mainittu kaksoisrooli. Toisaalta niin kyberrikostorjunnan kuin kyberturvallisuustilannekuvat tuottavat asiantuntijoille näkyvyyttä kybertoimintaympäristön tilanteeseen. Poliisille on turvattava riittävät kyvykkyydet rikosten ennalta estämiseksi ja esitutkinnan turvaamiseksi. Asiaan liittyy viranomaisten toimivaltuudet Yhteiskunnan turvallisuusstrategiassa mainituissa olosuhteissa ja poliisin näkökulmasta erityisesti normaaliolojen aikana. Toimivaltuuksiin liittyy olennaisesti tiedonvaihto viranomaisten välillä. Poliisi ei

esitutkintaviranomaisena jaa yksilöityä tietoa, mutta kyberrikostorjunnan ilmiötason tietoa on mahdollista hyödyntää kyberturvallisuuden ylläpitämisessä. Vastaavasti esitutkintavelvollisuus voi rajoittaa poliisin kyberrikostorjunnan ja tiedonvaihtoon osallistuvien toimijoiden yhteistyötä. Kyberrikostorjunnan suuntaamisessa voidaan kuitenkin hyödyntää tietoja, joita asiantuntijat saavat yhteistyöverkostojensa kautta.

Strategiassa mainitaan kansainvälisen yhteistyön vahvistavan Suomen kyberturvallisuutta. Tässä kohtaa on syytä huomioida ja painottaa, ettemme saa omalla lainsäädännöllämme ja tulkinnoilla vaikeuttaa yhteistyötä. Hyvä ja sujuva yhteistyö varmistetaan tarvittaessa lainsäädännöllisin keinoin. Tavoitteissa mainitaan, että monenvälinen yhteistyö on nyt ja tulevaisuudessa operatiivisen toiminnan keskeisin yhteistyömuoto. Kansallisella tasolla tulee mahdollistaa puitteet toimivalle kansainvälisten tietojen käsittelylle.

Strategiassa korostetaan kansalaisten osaamista ja ymmärrärrystä. Kansalaisten osaamisen varmistaminen kaikissa elämänvaiheissa luo perustan kyberturvalliselle toiminnalle kybertoimintaympäristössä. Kyberhygieniaa

on tuotu hyvin esille, mutta on erikseen arvioitava, onko tarvetta korostaa vaikeasti ymmärrettävällä käsitteellä asiaa vai voitaisiinko hyvien tietoturvakäytänteiden noudattamisella korvata tämä. Strategian kohta käsittelee kansalaisten osaamista, joten jo määritelmällisesti asiaan tulee suhtautua kohdeyleisön mukaisesti.

Kokkomäki Tuomas
Poliisihallitus