Poliisihallitus

Lausunto

06.01.2021 POL-2020-84538

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Yleisenä kommenttina voi todeta, että kokonaisuudessa on useita hyviä ehdotuksia poliittisiksi linjauksiksi, jotka tosiasiallisesti varmasti kehittäisivät tietoturvaa ja tietosuojaa yhteiskunnan kriittisillä toimialoilla. Useiden väliraportissa esitettyjen linjausten toteuttaminen voi edellyttää lisäresursseja julkishallinnolle. Ilman esim. taloudellisia lisäresursseja on, voi olla, ettei linjauksia olisi mahdollista toteuttaa julkishallinnossa nykyisillä rahoitus- ja henkilöstöraameilla.

Kohta 1. Viranomaisten välisen yhteistyön tiivistäminen on erittäin kannatettava toimenpide. Samalla on pidettävä huolta siitä, että lainsäädäntö mahdollistaa tiedonvaihdon eri viranomaisten välillä (esimerkiksi Traficomin Kyberturvallisuuskeskukselta tai tietosuojavaltuutetun toimistolta poliisille ja päinvastoin). Resurssien hyödyntäminen viranomaisten välillä ei saa myöskään johtaa siihen, että osaamis- ja resurssivajetta paikataan toisen viranomaisen resursseilla, jotka ovat sidottu viranomaisen ydintehtävien toteuttamiseen.

Kohta 2. Kyberturvallisuuskeskuksen resurssien vahvistaminen neuvonnan ja ohjauksen lisäämiseksi on kannatettavaa, mutta asiantuntijapalvelun perustaminen jokaiselle kriittiselle toimialalle vie merkittävän määrän henkilöresursseja. On huomattava, että Kyberturvallisuuskeskuksen resurssien vahvistaminen ei ainakaan merkittävästi vähennä tarvetta sille, että viranomaisissa on omat asiantuntevat ja riittävät resurssit tieto- ja kybertuvallisuustehtäviin.

Kohta 3. On pohdittava, että onko tarkoituksenmukaista, että Kyberturvallisuuskeskus olisi se taho, joka tarjoaa laajasti koulutusta sektoreiden tietoturvaa vastaaville viranomaisille vai tulisiko tässä hyödyntää yhteistyötä esimerkiksi korkeakoulujen kanssa. Henkilöstön vaihtuvuus kyberturvallisuuden parissa työskentelevillä henkilöillä on suuri, joten koulutusta olisi tarjottava säännöllisesti ja jo koulutetuille olisi tarjottava päivitettyä tietoa. On huomattava, että tällainen

yleinen koulutus ei ainakaan kaikilla toimialoilla poista tarvetta kyseisen toimialan erityispiirteet huomioivalle kohdennetulle koulutukselle.

Kohta 4. Olisi hyvä tietää mitä nämä kartoituspalvelut käytännössä tarkoittavat? Pelkkä skannauspalvelu ei välttämättä anna riittävää tietotaitoa haavoittuvuuksien korjaamiseksi. Tarvitaan myös asiantuntijapalvelua tulosten tulkitsemiseksi.

Kohta 5. Ehdotettu viranomaisten tarpeiden selvittäminen teknologisille ratkaisuille salassa pidettävien ja turvaluokiteltujen tietojen vaihtamiseen on syytä tehdä nopealla aikataululla, kuten myös sen perusteella tarvittavat jatkotoimenpiteet. Viranomaisten järjestelmien ja ympäristöjen välillä on tällä hetkellä eroavaisuuksia siten, ettei viranomaisilla ole toistaiseksi ollut turvallista tapaa mm. videoneuvotteluun ja tiedonvaihtoon. Viranomaisilla/julkisella sektorilla pitää olla kaikille sopiva tapa lähettää salattua sähköpostia tai muutoin välittää tiedostoja turvallisesti, ml. neuvottelujen käyminen sähköisin turvallisin välinein. Tällaisen yhteisen tavan puuttuessa kaikki sähköisen viestinnän käytetyt ratkaisut saattavat sisältää merkittävänkin tietoturvariskin. Luotavat järjestelmät on oltava sellaisia, että niiden käyttäminen ei vaadi käyttäjältä erityistä teknistä osaamista. Palveluntuottaja (Valtori) ja infrastruktuuri (sähköposti/pikaviesti) meillä jo on. Vain käytäntö puuttuu. Ainakin TL IV tasolle on kaikki edellytykset.

Kohta 6. Havaron käytön laajentaminen on kannatettava suositus. Samalla on pystyttävä konkreettisesti kuvaamaan Havaron käyttäjälle käytöstä tulevat hyödyt. Havaron käytön laajentamiselle tulee varmistaa myös riittävät resurssit, joko niin, että Havaroa tarjotaan julkishallinnolle keskitetyllä rahoituksella tai niin, että viranomaisille tai muulle julkiselle sektorille annetaan riittävät taloudelliset resurssit ko. havainnointi- ja varoitusjärjestelmän käyttöön.

Kohta 7. Ehdotamme täsmällisyyden vuoksi kohdan muokkaamista kuulumaan seuraavasti: Kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset lainsäädännössä. Viranomaisilla on oltava laissa säädetyt riittävät valtuudet antaa tietoturvaa koskevia sitovia määräyksiä kriittisille toimialoille. Olemassa olevat määräykset käydään läpi ja varmistetaan, että ne ovat ajan tasalla. Tietoturvavaatimusten valmistelussa huomioidaan kansallinen ja kansainvälinen lainsäädäntö ja niiden sen asettamat rajoitteet ja vaatimukset. Edellä oleva selventäisi kirjausta etenkin sen osalta, että kenelle määräyksiä tietoturvasta voitaisiin antaa, ei esim. kansalaisille.

Olisi tärkeää, että lainsäädännössä olisi määritelty tietoturvallisuuden tasot, jotka tulee jokaisen kriittisen toimialan järjestelmän täyttää perustuen järjestelmän tietosisältöön ja sen kriittisyyteen. Tämä tietoturvallisuuden tasoajattelu oli aiemmassa lainsäädännössä mukana ja velvoitti valtionhallinnon virastoja. Tämä voisi olla hyvä palauttaa takaisin käytäntöön ja ulottaa myös kriittisiin toimialoihin. Tasoajattelu tulisi kuitenkin rakentaa siten, että se mahdollistaa riskilähtöisen lähestymistavan tarkoituksenmukaisissakohdin (tarkemmin riskilähtöisyydestä kohtaa 8 koskevassa kirjauksessa alla).

Kohta 8. Toimialoille ehdotetaan säädettävän velvoite pyytää Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta lausunto tietoturvaa koskevista vaatimuksista ennen niiden hyväksymistä ja tarvittaessa myös vaatimusten toimeenpanosta. Tässä tulee huomioida riskiarviointi- ja -hallintalähtöisyys, jonka pohjalta on voitava tehdä tarvittavia poikkeamia. Liian kapea tulkinta (kyllä/ei) voi johtaa merkittäviin kustannuksiin ja voi monimutkaistaa järjestelmiä ja pahimmillaan jopa estää viranomaisia hoitamasta lakisääteisiä tehtäviään, eikä edes välttämättä paranna tietoturvaa.

Tällaisen toimintamallin myötä tulee myös arviointilaitosten määrää lisätä merkittävästi (kohta 13) ja huomioida tästä arviointitoiminnasta lisääntyvät kulut organisaatioille.

Mille toimialoille? Kaikille? Kohta kaipaisi selvennystä. Riittäisikö lausunnon sijaan se, että Kyberturvallisuuskeskus julkaisee eri aloja koskevat tietoturvavaatimukset ja nämä huomioidaan? Kohdan 8 voisi korvata kohta 9.

Kohta 10. Kohdassa ehdotettu velvoite prosessien ja toimintojen kuvaamiselle on pitkälti yhtenäinen velvollisuuden kanssa, joka tulee jo nykyään julkisen hallinnon tiedonhallinnasta annetusta laista (906/2019).

Kohta 11. Kohdassa ehdotetaan säädettäväksi velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. On hyvä, että kohdassa on otettu esiin tarve huomioida taloudelliset vaikutukset, jotka voivat olla merkittäviä. Näiden toteuttamiseen tulisi varmistaa riittävät henkilö- ja taloudelliset resurssit viranomaisille ja muille julkishallinnon toimijoille.

Kohta 12 ISO27001 sertifiointi on raskas prosessi. Tuo siirtymäaika on kohtalaisen lyhyt tuollaisen toteuttamiseksi.

Kohta 13 ehdottomasti kannatettava, jotta akkreditoinnit eivät kaadu siihen, ettei meillä ole tätä hoitavia tahoja.

Kohta 15 tietoturvavaatimukset pitäisi koskea myös kohtaa 14 sähköntuotannon osalta.

Kohta 18 poliisin toimivaltuuksien riittävyyden selvittäminen tietoverkkorikosten tutkimiseksi on kannatettava ja siinä on otettava huomioon nopeasti muuttuvan toimintaympäristön vaikutukset. Keskeistä tässä on toimivaltuuksien lisäksi riittävien tietojen saanti- ja käsittelyoikeuksien varmistaminen poliisille.

Kohta 19. Kohta on kannatettava. Poliisilla on oltava riittävät resurssit tietoverkkorikosten ennalta estämiseksi, paljastamiseksi ja tutkimiseksi. Tietoverkkorikosten selvittäminen vaatii erityistä asiantuntemusta. Tietoverkkorikokset ovat miltei aina rajat ylittäviä ja rikoksiin liittyy merkittävä määrä sähköistä todistusaineistoa, jonka hankkiminen ja käsittely sitovat paljon henkilöresursseja.

Kohta 20. Kannatettava. Viranomaisten ja eri toimijoiden ohjeistuksella voidaan lisätä tietoverkkorikoksista ilmoittamista ja tätä kautta parantaa tilannekuvaa vakavista tietoverkkorikoksista sekä tehostaa rikosvastuun toteutumista. Lisääntynyt tieto tietoverkkorikoksista mahdollistaa myös vastaavien tekojen ennalta estämisen. Törkeistä tietoverkkorikoksista ilmoittamatta jättämiselle ei ole hyväksyttävää syytä. Tärkeää on huolehtia myös siitä, että tieto tietoverkkorikoksesta saavuttaa poliisin ja muut viranomaiset mahdollisimman aikaisessa vaiheessa, jotta varmistetaan sähköisen todistusaineiston säilyvyys ja hyödynnettävyys rikostutkinnassa. Edellä olevaan liittyy myös kohta 35, jonka toteuttaminen olisi kannatettavaa ja mahdollistaisi tiedonvaihdon eri toimijoiden välillä.

Kohtien 22-26 ehdotuksia on poliisin arvion mukaan tarpeen edistää näillä toimenpiteillä saatavien selvien hyötyjen vuoksi. Valtorin tulee kyetä tarjoamaan valtion viranomaisille turvallisia ja tehokkaita välineitä ja palveluja kohtuullisin toimitusajoin.

Kohdassa 28 ehdotettu kyvykkyystason selvittämistä voidaan pitää kanna-tettavana toimenpiteenä kuin myös kohtien 30-32 ehdotuksia. On syytä huomata, että samoin kuin tietoturvasertifioinnit myös tietosuojasertifioinnit vaativat aikaa ja taloudellisia resursseja.

Kohta 33. Tietosuojavaltuutetun toimistolle riittävien resurssien varmistaminen on erittäin kannatettavaa. Nyt resurssien varmistaminen on ehdotuksessa kiinnitetty valvontatehtäviin ja loukkauksiin puuttumiseen. Henkilötietojen tietoturvaloukkausten ennalta estäminen on tarkoituksenmukaista aina, kun mahdollista, joten myös ohjaustyöhön (esim. ennakkokuulemismenettely, yleinen neuvonta) ja muihin tehtäviin, jotka tietosuojavaltuutetun toimistolle kuuluvat, tulisi varmistaa riittävät resurssit.

Esitämme harkittavaksi, että olisi poliittisissa linjausehdotuksissa tai muutoin raportissa hyvä huomioida myös tieto- ja kyberturvallisuuden harjoitustoiminnan tärkeys. Tulisiko harjoitteluun kriittisillä toimialoilla toimivia velvoittaa tai kohdistaa vahva suositus tähän liittyen? On hyvä huomata, että myös harjoitustoiminta vaatii niin henkilö- kuin taloudellisia resursseja.

Väliraportin muut osat, kommentit:

Poliisihallitus haluaa vielä tuoda esiin, että olisi tärkeää kaiken kaikkiaan luoda yhteinen vaatimuskehikko eritasoista tietoa sisältäviin tietojärjestelmiin sekä yhtenäinen säädöspohja kriittisten toimialojen tietojärjestelmien tietoturvavaatimuksille, jonka avulla harmonisoidaan myös hankintoja ja joka yleistyessään parantaisi tuottajien kyvykkyyttä tietoturvallisten järjestelmien kehityksessä yleisemminkin.

Vaikka turvallisuusviranomaisten ns. TUVE-kokonaisuus on rajattu tämän arviointi- ja kehitystyön ulkopuolelle, se tulisi myös tarkastella ja kyetä integroimaan tähän kokonaisuuteen mukaan.

Lopuksi toteamme merkittävänä havaintona, että muistion lopussa oleva arvio henkilöstön lisäystarpeesta ei sisällä sisäministeriön osiota eli esimerkiksi tietoverkkorikosten tutkintaan ja ennalta estämiseen liittyviä resursseja ei ole tämän raportin mukaan tarve lisätä lainkaan. Poliisihallitus katsoo, että riittävien henkilöresurssien varmistaminen myös kyberrikostorjuntaan ja -tutkintaan sekä tietoverkkorikollisuuden paljastamiseen edesauttaisi myös kriittisten toimialojen tietoturvallisuutta ja tietosuojaa.

Hautala Annina
Poliisihallitus