

Martti Setälä

Liikenne- ja viestintäministeriö

[Viite]

Kuntaliiton sekä Jyväskylän, Lappeenrannan ja Porin kaupunkien ja Utajärven kunnan lausunto Suomen kyberturvallisuusstrategiasta

Johdanto

Luonnos Suomen kyberturvallisuusstrategiaksi on tasapainoinen ja laadukkaasti laadittu sekä tarjoaa nykymuodossaan hyvät lähtökohdat Suomen kyberturvallisuuden kehittämiseksi pitkällä aikavälillä. Tavoitetilakuvaus on hyvä ja kattava.

Lausunnon antajat esittävät tarkennuksia dokumenttiin kansallisen kybersietoisuuden, sidosryhmien välisen yhteistyön edellytysten ja kyberturvallisuuden kehittämistoimenpiteiden vaikuttavuuden varmistamiseksi.

Yleisissä havainnoissa on kirjattu keskeisimmät strategialuonnoksen kehittämissuositukset kuntakentän näkökulmasta. Yksityiskohtaisissa havainnoissa kehittämissuosituksia on tarkennettu ja ehdotettu konkreettisia kirjauksia.

Kuntaliitto haluaa kiinnittää huomiota siihen, että kyberstrategialuonnoksen valmistelutyössä siitä vastannut sihteeristö on pyrkinyt osallistamaan mukaan paikallishallinnon edustajat ja että valmistelutyö - siltä osin kuin paikallistaso on saanut osallistua siihen - on tapahtunut hyvässä yhteistyössä ja -hengessä.

Yleiset havainnot

- Julkiselle hallinnolle kuten paikallishallinnolle tulee tarjota jatkossakin kansallisen tahon kehitysrahoitusta digitalisaation ja



kyberturvallisuuden ratkaisujen kehittämiseen ja riittävä kyberturvallisuuden perusrahoitus tulee varmistaa koko paikallishallinnon toimijakentälle.

- NIS2:n toimeenpano vie jatkossa suuren osan kansallisten kyberturvallisuutta ohjaavien ja kehittävien viranomaisten huomiosta. NIS2:n soveltamisalan ulkopuolelle jää kuitenkin merkittävä osa julkisen hallinnon toimijoista. Tulee varmistaa, että niiden kyberturvan kehittäminen saa riittävästi huomioita kansallisella agendalla. Tiedonhallintalain nykyisen 4. luvun velvoitteiden jalkautukseen julkisen hallinnon toimijakentässä tulee varata jatkossakin kansalliselta tasolta riittävä tuki, suositukset ja työkalut.
- Kyberturvallisuusympäristöä koskevan tiedon vaihdon edellytyksiä kehitettäessä (lainsäädäntö, toimintamallit ja työvälineet) tulee varmistaa paikallistason toimijoille riittävät edellytykset osallistua kaksisuuntaiseen tiedonvaihtoon ja tilanneymmärryksen muodostamiseen.
- Palveluiden ja toimitusketjujen turvaamisessa tulee edelleen ja entistä vahvemmin pyrkiä ”sisäänrakennettuun turvallisuuteen” ja turvallisuuden varmistamiseen kansallisen tason toimenpitein.
- Kansallisissa hankkeissa kehitettyjen ja vaikuttavaksi arvioitujen julkisen hallinnon yhteisten digiturva-/kyberturvapalveluiden (esimerkiksi HYÖKY, Havaro, organisaation kyberturvakysely ja yhteisesti tuotetut koulutusaineistot sekä kyberharjoitukset) rahoitus ja resursointi tulee varmistaa pitkällä aikajänteellä.
- Kyvykkyys tunnistaa, kehittää ja tuottaa uusia yhteisiä ja kansalliselta tasolta rahoitettuja julkisen hallinnon yhteisiä digiturva-/kyberturvapalveluita tulee ylläpitää pitkäjänteisesti.
- Tietoturva- ja tietosuojatoimijoiden, agendojen ja ratkaisujen läheinen yhteys tulee varmistaa pitkäjänteisesti, ja tulisi siksi kirjata selvästi esiin myös tähän tavoitedokumenttiin.
- Perusteettomien uusien tehtävien sekä pakottavan lainsäädännön ja vaatimusten osoittamista kuntakentälle tulee välttää. Uuden lainsäädännön tulee olla lähtökohtaisesti mahdollistavaa (ei pakottavaa).

Yksityiskohtaiset havainnot

Johdanto – kyberturvallisuus osana kokonaisturvallisuutta

- Dokumentissa voisi olla nykyistä paremmin avattuna EU:n kyberturvallisuuspolitiikan ja lainsäädäntötyön keskeiset pitkän aikavälin tavoitteet sekä niiden vaikutukset kansallisiin ratkaisuihin.

Toimintaympäristön muutos

- s. 13, 2 kappale: lisäsehdotus tekstiin (jotenkin olisi huomioitava se, että NIS2 sääntely koskee vain suuria toimijoita ja hallinnosta vain valtio ja aluetasojä):
 - ”Useiden julkisen hallinnon toimijoiden kyberturvallisuuden kehittäminen perustuu jatkossakin ennen NIS2:ta säädettyihin tiedonhallintalain tietoturvakäytäntöihin sekä niiden toimeenpanoa tukeviin järjestelyihin. Näiden säädösten aktiivinen ylläpitäminen ja järjestelyiden jatkuvuus tulee turvata.”
- s. 14, 2 kappale: lisäsehdotus nykyisen tekstin oheen:
 - ”Sujuva tiedonvaihto julkisen hallinnon valtio-alue-paikallis tason toimijoiden välillä on tärkeää ja sen edellytyksiä tulee parantaa.”

Nykytila

- s. 18, kappale 2: Kuntakenttään liittyvää mainintaa voisi päivittää korvaamalla sen tällä tekstillä.
 - ”Verrattuna valtion- ja aluehallintoon, paikallishallinnon kyberturvallisuuden kokonaistaso on niitä hieman heikompi. Kyberturvan tasossa on kuitenkin kuntakentän toimijoiden välillä eriytymistä, joka johtuu muun muassa eroista kuntien ja niiden palveluntoimittajien kanssa ja resursseissa. Esimerkiksi suurimmat kaupungit ovat pääsääntöisesti korkealla kyberturvan tasolla.”
- s 18, Kappale 3: Sisältöä kannattaisi päivittää (lisäsehdotukset hakusulkeissa)
 - Hyvinvointialueet ja kunnat tarvitsevat kyberturvallisuuden varmistamisessa nykyistä enemmän tukea, kuten keskitettyjä kyberturvallisuuspalveluja [sekä yhteisten kyberturvallisuuspalveluiden hyödyntämisen ja lainsäädännön vaatimusten toimeenpanon ennakoivaa neuvontaa ja muuta mahdollista käytännön tukea].

- Kyberuhkiin vastaamisen on toimittava saumattomasti eri koosten toimijoiden välillä ja ajallisesti portaattomasti niin valtakunnallisesti kuin alue- ja paikallistasollakin. [Tämän mahdollistamiseksi tulee olla tehokkaat yhteistyö- ja verkostorakenteet sekä edellytykset jakaa tilannetietoja ja ylläpitää yhteistä tilannekuvaa.]
- Kyberhäiriöiden aiheuttamat vahingot voivat olla sellaisia, ettei niitä pystytä täysin korvaamaan esimerkiksi tietojen tuhouttua tai vuodettua pysyvästi. Jotkin pienet yritykset ovat jopa joutuneet lopettamaan toimintansa kyberturvallisuusriskien toteuduttua. [Vastaavasti julkisten palveluiden tietovuotojen hintaa on vaikea määritellä, mutta niiden vaikutukset yleiseen kansalaisluottamukseen ja tietovuodon asianomistajien hyvinvointiin voivat olla mittavia.] Tämä korostaa entisestään riittävien resurssien kohdentamista kyberturvallisuuteen sekä yhteistyön ja yhteisten menettelytapojen tärkeyttä.

Pilarit ja niiden strategiset tavoitteet

Pilari I: Osaaminen, teknologia ja TKI

- s 23, Kappale 2: Ehdotus lisäyksiksi tekstiin hakasulkeissa:
 - Yritysten [sekä julkisen ja kolmannen sektorin organisaatioiden] vastuulliseen toimintaan kuuluu kehittää kyberturvallisia kyvykkyksiä, tunnistaa uhkat, reagoida haitalliseen toimintaan ja ilmoittaa häiriöistä kybertoimintaympäristössä. [Varhaiskasvatuksessa,] kouluissa, [oppilaitoksissa ja korkeakouluissa] opettajien valmiuksia kasvattaa oppilaita [ja opiskelijoita] kriittiseen medialukutaitoon sekä tietoisuuteen [arjen ja työelämän] kyberriskeistä [ja niiden hallintakeinoista] on vahvistettava laajan yhteiskunnallisen resilienssin lujittamiseksi. [Sama koskee aikuisen kansalaisosaamisen edellytyksiä kehittävää vapaata sivistystyötä.] Kokonaisuudessaan suomalainen kyberturvallisuusosaaminen varmistetaan vahvistamalla kyberturvallisuuden roolia laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla.

Pilari II: Varautuminen

- s 27, Kappale 1: Lisäsehdotus tekstiin hakasulkeissa:
 - Toimivuuden varmistamisessa ja häiriönsietokyvyn kehittämisessä tärkeää on erityisesti [varmistaa, ettei resursseja prosesseja ole viritetty liian tehokkaiksi, jolloin usein katoaa kyky muokautua nopeisiin muutoksiin, eli resilienssi. Toisin sanoen toiminnassa tulee olla riittävästi ”väljyyttä”. Perustietoturvatyön resursoinnin tuleekin olla riittävällä tasolla. Lisäksi vaatimusten mukaisuuden toteutumista tulee arvioida ja seurata jatkuvaluonteisesti erilaisilla arvioinneilla ja tarkastuksilla sekä testauksilla ja harjoituksilla. Esimerkiksi] hyödyllistä olisi

kyberharjoittelun kehittäminen ja ulottaminen entistä laajemmalle huomioiden palvelu- ja toimitusketjujen kyberturvallisuus sekä erilaiset keskinäisriippuvuudet.

- s. 27, Kappale 2: Ehdotus lisättäväksi tarkentavaksi tekstiksi soveltuvaan paikkaan (esim. uusia kappaleita em. perään):
 - ”Palveluiden ja toimitusketjujen turvaamisessa tulee edelleen ja entistä vahvemmin pyrkiä ”sisäänrakennettuun turvallisuuteen” ja turvallisuuden varmistamiseen kansallisen tason toimenpitein esim. velvoittamalla, valvomalla ja arvioimalla palveluntarjoajia ja toimitusketjuja. Tavoitteena on, että palveluita hankkivat julkisen hallinnon toimijat voivat olla nykyistä varmempia palveluiden riittävän tasoisesta tietoturvasta ja tietosuojasta jo ostaessaan palvelut. Myös tietoturva- ja tietosuojan arviointeja tulee tehdä selvästi nykyistä enemmän keskitetysti, vaikka lopullinen vastuu ei poistuisikaan tiedonhallintayksiköiltä (kuten kaupunki, hyvinvointialue tai virasto). Hyvä esimerkki tästä on vaikuttaminen suurikokoisiin kansainvälisiin ja kansallisiin pilvipalveluiden toimittajiin ja niiden sopimusehtoihin.”
- s. 28, Kappale 3: Lisäsehdotus tekstiin hakasulkeissa
 - Kyberrikosten ennalta estämistä on tuettava lainsäädännöllä, joka mahdollistaa tiedon jakamisen viranomaisten ja yritysten [sekä alue- ja paikallishallinnon toimijoiden] kesken.
- s. 29, Kappale 1: Ehdotus sanan poistamiseksi ja kahden sanan lisäämiseksi virkkeen ymmärrettävyyden parantamiseksi. Ehdotukset hakasulkeissa.
 - ”Lisäksi alue- ja paikallishallinnossa on edistettävä [POIS: yhteisten, TILALLE: soveltuvalta osin] kyberturvallisuustehtävien keskittämistä päällekkäisen työn välttämiseksi ja resurssien käytön tehostamiseksi.”
- s. 29, Kappaleet 4-5: Ehdotus lisäykseksi tekstiin soveltuvaan kohtaan:
 - ”Yhteisen, kansallisen harjoitustoiminnan kehittämisessä ja tarjonnassa huomioidaan tasapuolisesti hallinnon tasot (valtio-alue-paikallinen).”

Pilari III: Yhteistoiminta

- s. 32, Kappale 3: Ehdotus lisäykseksi tekstiin hakasulkeissa:
 - Suomi vaikuttaa aktiivisesti EU:n kyberturvallisuuspolitiikan- ja sääntelyn kehittämiseen ja vie omaa kansallista kokonaisturvallisuuteen ja ennakkolliseen varautumiseen pohjautuvaa malliaan unioniin ja muihin jäsenmaihiin. [Hyödynnetään mallin viennissä kaikkien kansallisen ekosysteemin keskeisten sidosryhmien kansainvälisiä verkostoja.]
- s. 34, Kappale 1: Ehdotus lisäykseksi tekstiin [hakasulkeissa]
 - Korkeasti turvallisuusluokitellun tiedon jakaminen edellyttää siihen soveltuvien järjestelmien kehittämistä ja käyttöönottoa [sekä tarvittaessa uusien tietojärjestelmien järjestämisratkaisujen toteuttamista].

- Oman alaotsikkonsa alle olisi hyvä kirjata huomiot tietosuojan yhteydestä kyberturvallisuuteen sekä tietoturva- ja tietosuojatyön koordinaatiosta ja sen tavoitteista
 - Taustaksi: Aiemmalla strategiakaudella valtioneuvoston periaatepäätöksissä julkisen hallinnon digitaalinen turvallisuus ja tietoturvallisuuden ja tietosuojan kehittämiseksi yhteiskunnan kriittisillä toimialoilla (Titukri) huomioitiin tämä yhteys ja sitä tiivistettiin erinäisin toimenpitein kuten laatimalla ja julkaisemalla julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri). Jatkossa tietoturvan ja tietosuojan yhteyttä tulisi ylläpitää ja vahvistaa esimerkiksi huomioimalla jatkossakin ne yhdessä arviointikriteeristöissä ja yhteensovittamalla tietoturvan ja tietosuojan riskinarviointi-, sertifiointi- ja arviointilaitosten hyväksymisprosesseja.

Resursointi, toimeenpano ja seuranta

- s. 42, kappale 1: Lisäysehdotukset tekstiin sopivaan kohtaan:
 - "Kyberturvallisuuden riskien ja jatkuvuudenhallintaa sekä varautumista tulee toteuttaa saumattomasti osana organisaatioiden kokonaistason riskien ja jatkuvuudenhallinnan sekä varautumisen prosesseja."
- s. 42, kappale 2: Lisäys tekstiin:
 - "Eri toimijoiden (mukaan lukien julkisen hallinnon viranomaiset) toteuttamaa tutkimus- ja selvitystoimintaa on koordinoitava ja yhteensovitettava entistä paremmin. Yhteistyötä on myös tiivistettävä sidosryhmäraajat ylittäen kansainvälisten, erityisesti EU:n tarjoamien, rahoitusmahdollisuuksien hyödyntämiseksi."
- s. 42, kappale 3: Lisäysehdotus tekstiin hakasulkeissa:
 - Tämä edellyttää Suomelta vastinrahaa ja hallinnonalojen [sekä -tasojen] välistä resurssien käytön koordinoitua.
- s. 43, kappale 1: Lisäysehdotus tekstiin sopivaan kohtaan:
 - "Seurannassa huomioidaan strategian toteutuminen julkisen hallinnon eri tasoilla (valtio-alue-paikallinen)."
 - HUOM! Tarvittaessa päivitettävä kappaleen tekstikirjausta siten, että kooste on mahdollista jakaa tiedoksi myös alue- ja paikallistason viranomaisille.
- s. 43, kappale 2: Lisäysehdotus tekstiin sopivaan kohtaan:
 - "Seurannassa huomioidaan soveltuvalta osin strategian toteutuminen julkishallinnon alue- ja paikallistasoilla. Lisäksi alue- ja paikallistason viranomaisten edustajia kuullaan toimeenpanosuunnitelman laatimisen ja vuosittaisen arvioinnin yhteydessä."

Strategiset kehittämissuhteet

- s. 44-45: Lisäysehdotukset uusiksi strategisiksi kehittämissuhteiksi

- ”Lisättävä hallitusti kaikilla toiminnan tasoilla kyberturvallisuuden resursointia.”
- ”Tuotettava soveltuvalta osin julkiselle hallinnolle yhteiset kyberturvapalvelut keskitetysti kansalliselta tasolta.”
- ”Päivitettävä yhteistä lain tulkintaa ja yhteisiä toimintamalleja kyberturvallisuustoimenpiteiden tuottavuuden ja vaikuttavuuden varmistamiseksi.”

Liitteet: Kyberturvallisuuden kansallinen yhteistoimintamalli

- s. 51, kappale 2: Lisäysehdotus hakasulkeissa:
 - Toimijoihin kuuluvat valtion virastot, liikelaitokset ja yhtiöt, aluehallinnon toimijat, hyvinvointialueet, kunnat ja kuntayhtymät, [hyvinvointialueiden ja kuntien omistamat in house -yhtiöt] sekä julkiset palveluntuottajat ja itsenäiset laitokset.

Termit

- Kannattaisiko ”Termit” osio nimetä uusiksi nimellä: ”Sanasto”?

—

Annamme mieluusti lisätietoja lausunnostamme. Yhteyshenkilönä toimii Kuntaliiton erityisasiantuntija Martti Setälä.

LAUSUNNON ANTAJAT

Jyväskylän kaupunki
Lappeenrannan kaupunki
Porin kaupunki
Utajärven kunta
Suomen kuntaliitto ry

Jakelu Lausuntopalvelu.fi

Tiedoksi Kuntien Tietoturavastaavien verkosto, Kuntien tietosuojavastaavien verkosto, Turvallinen ja kriisinkestävä kunta verkosto, Kaupunkien tietohallintojohtajien verkosto, Hyvil Oy ja Kustos Ry.