7.4.2022 D/727/04.07.02/2021, 185/54/2016

Jakelussa mainitut

Tuloksellisuustarkastuskertomus 16/2017: Kybersuojauksen järjestäminen, annettu 5.10.2017
Jälkiseurantaraportti 16.1.2020

Jälkiseurantaraportin 16.1.2020 täydennys

Valtiontalouden tarkastusvirasto on täydentänyt 16.1.2020 päivättyä jälkiseurantaraporttia jatkoseurannalla, joka koskee kybersuojauksen järjestämistä. Jälkiseurannan jatkamisesta oli tehty päätös 27.1.2020.

1 Jatkoseurannan toteutus

Kybersuojauksen järjestämistä koskeneessa tarkastuksessa (16/2017) tarkastusvirasto arvioi, onko valtionhallinnon kybersuojaus järjestetty mahdollisimman vaikuttavasti ja taloudellisesti tarkoituksenmukaisella tavalla. Tarkastuskertomuksessa tarkastusvirasto suositti, että valtiovarainministeriö kehittää laajavaikutteisiin kyberhäiriötilanteisiin operatiivisen hallinta- ja johtamismallin. Tarkastusvirasto pyrki suosituksillaan edistämään myös sitä, että valtion talousarvion määrärahat kohdistuisivat kybersuojauksen kokonaisuuden kannalta tärkeimpiin kohteisiin ja turvaisivat Kyberturvallisuuskeskuksen toiminta-edellytykset. Lisäksi suositukset koskivat kyberloukkauksista ilmoittamisen nykyistä vahvempaa velvoittavuutta ja Valtion tieto- ja viestintätekniikkakeskus Valtorin kybersuojauksen menettelyjä.

Tammikuussa 2020 valmistuneessa tarkastuksen jälkiseurannassa havaittiin, että valtiovarainministeriö ei ollut määritellyt valtionhallinnon ICT-palvelujen operatiivista hallinta- ja johtamismallia. Muualla valtionhallinnossa kehitetyn kyberturvallisuusjohtaja-mallin katsottiin kuitenkin vahvistavan ICT-palvelujen hallintaa laajavaikutteisissa kyberhäiriötilanteissa. Jälkiseurannassa valtiovarainministeriö ei pitänyt tarpeellisena muuttaa kybersuojaukseen liittyviä budjettimenettelyjä. Ministeriö ei myöskään toistaiseksi nähnyt perusteita sille, että kyberloukkauksista ilmoittaminen Kyberturvallisuuskeskukseen tehtäisiin velvoittavaksi. Valtori oli antamansa selvityksen perusteella toteuttanut sille osoitettua suositusta asianmukaisesti.

Tarkastusvirasto katsoi tarpeelliseksi täydentää jälkiseurantaa jatkoseurannalla.

Jatkoseurannassa pyydettiin valtiovarainministeriötä vastaamaan seuraaviin kysymyksiin:

1. Onko ministeriö määritellyt ja toteuttanut valtionhallinnon ICT-palveluiden osalta laajavaikutteisten kyberhäiriötilanteiden operatiivisen hallinta- ja johtamismallin?
2. Onko ministeriö selvittänyt, miten palveluiden kybersuojaus tulisi ottaa huomioon palveluiden koko elinkaaren rahoituksessa?
3. Onko ministeriö parantanut kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle?

Jatkoseuranta oli suunniteltu toteutettavaksi tarkastuskohteelle lähetettävällä selvityspyyntökirjeellä 16.1.2022 mennessä. Jatkoseuranta toteutettiin joulukuun 2021 ja tammikuun 2022 aikana. Selvityspyyntö lähetettiin valtiovarainministeriölle 8.12.2021 ja vastaus saatiin 21.1.2022.

Jatkoseurannan yhteydessä on perehdytty valtioneuvoston periaatepäätöksenä julkaistuun ”Kyberturvallisuuden kehittämisohjelma”-julkaisuun (10.6.2021) ja haastateltu valtion kyberturvallisuusjohtajaa, joka on vastannut kehittämisohjelman valmistelusta. Jatkoseuranta toteutettiin suunnitelman mukaisesti.

2 Jatkoseurannan uudet havainnot

2.1 Valtiovarainministeriö määrittelee ja toteuttaa valtionhallinnon ICT-palveluihin laajavaikutteisten kyberhäiriötilanteiden operatiivisen hallinta- ja johtamismallin

Valtiovarainministeriö on kuvannut jatkoseurantaa varten antamassaan selvityksessä Valtorin tietoturva- ja kyberturvallisuuspalveluita. Niiden tarkoituksena on turvata muiden palveluiden tietoturvallisuus, saatavuus ja käytettävyys ympärivuorokautisella valvonnalla, reagoimalla tietoturvauhkiin ja poikkeamiin sekä ennaltaehkäisemällä mahdollisia tulevia häiriötilanteita. Ministeriön selvityksessä todetaan, että häiriötilanteissa Valtorin tietoturva- ja kyberturvallisuuspalveluiden tehtävänä on suorittaa korjaavat ensitoimenpiteet, hälyttää tarvittaessa lisäresursseja paikan päälle ja vastata huolto- ja häiriötilannetiedottamisesta.

Valtiovarainministeriön mukaan uutta julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallia on tarkoitus kehittää osana meneillään olevaa Julkisen hallinnon digiturva 2020–2023 (Haukka) -hanketta. Mallissa tullaan määrittelemään mm. ”operatiivisen johtamisen vastuut ja järjestelyt, huomioiden viranomaisten toimivaltuudet”. Kunta–valtio-yhteistoimintamallia käsittelevä esiselvitys julkaistiin 11.6.2021, ja tehtävän jatkoon on ministeriössä asetettu koordinaatioryhmä. Ryhmän tehtävänä on siis kuvata yhteistoiminta- ja hallintamalli. Koordinaatioryhmän tavoitteena on tuottaa selvitysraportti, joka luo perustan mahdolliselle säädösvalmistelulle. Selvitysraportin on tarkoitus vastata myös valmistelussa olevaan, tarkistettuun verkko- ja tietoturvadirektiiviin (ns. NIS2-direktiiviehdotus). Direktiivin mukaan jäsenvaltioiden tulisi määritellä yksi tai useampi valvova viranomainen, joka on vastuussa laajamittaisten kyberturvallisuushäiriöiden ja -kriisien operatiivisesta johtamisesta.

Edellä kuvatun lisäksi valtiovarainministeriö on tuonut selvityksessään laajasti esille muita tietoturvaa yhtenäistäneitä ja kyberturvallisuuden harjoitustoimintaa vahvistaneita toimia, kuten:

- laki julkisen hallinnon tiedonhallinnasta (906/2019) sekä siihen liittyvät lait ja niiden toteutumista valvomaan perustettu Tiedonhallintalautakunta
- tiedonhallinnan yhteistyöryhmien perustaminen
- kyberturvallisuuteen liittyvien hankkeiden rahoitus ja toiminnan tulosohjaus (valtionhallinnon GovCERT-palveluiden jatkokehitys, Haukka-hanke, JUDO-hanke, Valtorin tulossopimukseen liittyvät kehittämisohjelma ja kehittämishankkeet)
- kyberturvallisuuden harjoitustoiminnan suunnitteluun ja ohjaukseen osallistuminen (KYHA-kyberturvallisuusharjoitukset)
- häiriötilanneohjeistuksen laatiminen palveluntuottajille (käsitellään tarkemmin luvussa 2.3)

Valtiovarainministeriön esille tuomat toimet ovat kuitenkin enemmän kybersuojauksen strategista kehittämistä kuin operatiivisia vastuita määrittäviä tai täsmentäviä.

Valtiovarainministeriön selvityksen perusteella laajavaikutteisten kyberhäiriötilanteiden operatiivinen hallinta ja niihin liittyvä viestintä jäävät nykytilanteessa palveluntuottajan vastuulle osana muuta asiakasyhteydenpitoa. Suunnitteilla olevan julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin toteutuminen selvityksessä kuvatulla tavalla edistäisi tarkastusviraston antamaa suositusta. Tätä voisi pitää myönteisenä, joskin tarkastukseen nähden myöhäisenä kehityksenä.

2.2 Valtiovarainministeriö selvittää, miten palveluiden kybersuojaus tulisi ottaa huomioon palveluiden koko elinkaaren rahoituksessa

Valtiovarainministeriön jatkoseurantaa varten antaman selvityksen mukaan kybersuojaus otetaan edelleen huomioon hankearvioinneissa, ja tiedonhallintalain (906/2019) lausuntomenettelyä koskeva

ohjeistus korostaa kybersuojauksen huomiointia osana palveluita ja toimintaa. Ohjeistuksessa olevassa mallipohjassa pyydetään arvioimaan myös tietoturvallisuuden ja varautumisen taloudellisia vaikutuksia.

Valtiovarainministeriö toi jatkoseurannassa esille myös Vahti-toiminnan ohjauksen siirtymisen virastotasolle ja Digi- ja väestötietoviraston Julkisen hallinnon digitaalisen turvallisuuden (JUDO) -hankkeessa rakenteilla olevan kokonaiskuvapalvelun. Palvelussa organisaatiot voisivat seurata oman digitaalisen turvallisuuden hallinnallisen tilanteensa kehittymistä sekä vertailla tilannetta muihin organisaatioihin. Tämä mahdollistaa valtiovarainministeriön mukaan rajallisten kehittämisresurssien tarkoituksenmukaisen kohdentamisen ja kehittämistoimenpiteiden vaikuttavuuden seurannan. Julkisen hallinnon johto voisi puolestaan seurata kokonaistilanteen kehittymistä, mikä ministeriön mukaan mahdollistaa tarkoituksenmukaisten kehittämistoimenpiteiden käynnistämisen. Ministeriö on myöntänyt Digi- ja väestötietovirastolle vuosiksi 2022–2023 kokonaiskuvapalvelun täydentämiseen 225 000 euroa.

Rahoitukseen liittyen valtiovarainministeriö on kuvannut selvityksessään käynnissä olevia digitaalisen turvallisuuden hankkeita. Haukka-hanketta on rahoitettu yhteensä noin neljällä miljoonalla eurolla vuosina 2020–2023, kyberturvallisuuden kehittämisohjelman toimeenpanoa kuudella miljoonalla eurolla vuosina 2021–2022 (rahoituksesta viisi miljoonaa euroa on EU:n RFF-rahoitusta) ja tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla -periaatepäätöksen toimeenpanoa noin neljällä miljoonalla eurolla vuonna 2022.

Lisäksi valtiovarainministeriö ohjasi Valtoria vuoden 2021 keväällä toteuttamaan ulkopuolisen tietoturva-arvion ja ryhtymään toimenpiteisiin. Valtorin tietoturvapalveluiden korjausvelka ja kehittämiskohteiden painopiste kohdistuvat erityisesti TORI-liiketoimintaan, mutta molemmilla (TORI ja TUVE) liiketoiminta-alueilla yhteisiä kehityskohteita ovat jatkossakin verkon havainnointi- ja hyökkäyksenestopalvelut ja pilvipalveluiden tietoturvallisuus.

Valtiovarainministeriön julkisen hallinnon ICT-osasto (JulkICT) on käynyt keskustelua lisärahoituksesta sekä TORI- että TUVE-liiketoiminta-alueille tieto- ja kyberturvallisuuden parantamiseen vuosina 2023–2026 valtiontalouden kehysvalmistelujen yhteydessä (VN/19255/2021). Tarvittavan rahoituksen määräksi on arvioitu 3 670 000 euroa vuonna 2023. Keskustelussa on todettu, että esitettyjen toimenpiteiden toteutuksen lykkääminen voi vaarantaa Valtorissa vaatimustenmukaisen palvelutuotannon. Se voi myös kasvattaa korjausvelkaa niin, että palveluiden laatu heikkenee ja niiden vertailtavuus markkinatoimijoiden vastaaviin palveluihin heikkenee entisestään.

Valtorin tietoturva- ja kyberturvallisuuspalveluiden kehittäminen tullaan jatkossa rahoittamaan asiakasmaksujen kautta, mikä aiheuttaa virastoille tarpeen esittää kehyksen ylittävää rahoitusta. Valtori arvioi omassa kehysehdotuksessaan vuosille 2023–2026, että esimerkiksi kustannusvaikutuksen kohdistuminen edellä mainituissa kehittämishankkeissa vuonna 2023 pelkästään asiakasrahoitteiseksi nostaisi Valtorin TORI-asiakasmaksuja 3–4 prosenttia ja TUVE-asiakasmaksuja 7 prosenttia. Tämä voi näkyä lisätalousarvioesityksinä erityisesti vuonna 2023.

Valtiovarainministeriön selvityksessään esille tuomaa lausuntomenettelyä on tarkasteltu tiedonhallinnan lainsäädännön kehittämisen eri vaiheissa. Tarkastusvirasto julkaisi vuonna 2015 Yhteentoimivuus valtion ICT-sopimuksissa (7/2015) -tuloksellisuustarkastuksen, jonka mukaan lausuntomenettelyllä ei vielä tuolloin kyetty antamaan vaikuttavia lausuntoja tietojärjestelmähankinnoista tai ottamaan kantaa siihen, tehdäänkö hallinnossa päällekkäistä kehitystyötä. Lausuntomenettelyn nykyisestä vaikuttavuudesta olisi hyvä saada tarkempaa tietoa. Kybersuojauksen rahoituksen epävarmuutta lisäävinä seikkoina jatkoseurannassa havaittiin Valtorin korjausvelan kasvu ja Valtorin tietoturva- ja kyberturvallisuuspalveluiden asiakasrahoitteisuus. Korjausvelan kasvun voidaan katsoa liittyvän pirstaleiseen, hankkeiden kautta tapahtuvaan kybersuojauksen rahoitukseen. Tarkastusvirasto pyrki tarkastuksen suosituksellaan korostamaan erityisesti sitä, että kybersuojaus on osa jatkuvaa toimintaa, jota pitäisi rahoituksella pystyä tukemaan pitkäjänteisemmin. Korjausvelkaan kohdistuvana toimena Valtiontalouden tarkastusvirasto käynnistää tarkastuksen vanhoista tietojärjestelmistä kevään 2022 aikana.

Jatkoseurannassa saadun selvityksen perusteella voidaan todeta, että hankerahoitus vastaa vain osin tarkastuksen suositukseen. Lausuntomenettely ja valmisteilla oleva kokonaiskuvapalvelu voivat onnistuessaan viedä kybersuojauksen rahoitusta suosituksen osoittamaan suuntaan.

2.3 Valtiovarainministeriö parantaa kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle

JulkICT-osasto on 20.9.2021 antanut palveluntuottajille (Valtori, Digi- ja väestötietovirasto, Suomen Erillisverkot Oy) ohjeen aiheesta ”Ensitiedon ilmoittaminen valtiovarainministeriölle valtion yhteisten tieto- ja viestintäteknisten ja julkisen hallinnon yhteisten sähköisten asioinnin tukipalvelujen häiriö- ja uhkatilanteissa” (VN/17213/2021). Ohje on laadittu varmistamaan sujuva sisäinen ensitiedonkulku häiriö- ja uhkatilanteissa, ja siinä kuvataan palveluntuottajien vastuu ilmoittaa korkean prioriteetin ja keskitason prioriteetin häiriötilanteista Kyberturvallisuuskeskukselle.

Valtiovarainministeriö on selvityksessään arvioinut Valtorin ja Digi- ja väestötietoviraston häiriötilanteisiin liittyvää yhteydenpitoa Kyberturvallisuuskeskukseen tiiviiksi. Digi- ja väestötietovirastolla on käytössä muun muassa poikkeamienhallintaprosessi, jonka mukaan he ilmoittavat virastoon kohdistuvista vakavista tietoturvapoikkeamista aina Kyberturvallisuuskeskukselle. Valtiovarainministeriön Kyberturvallisuuskeskukselta saamien tietojen mukaan kokonaisuutena valtionhallinnon ja Kyberturvallisuuskeskuksen välinen tiedonvaihto on parantunut viime vuosien aikana. Valtiotoimijat ovat tehneet kuukausittain 16–145 poikkeamailmoitusta Kyberturvallisuuskeskukselle vuosina 2019–2021.

Lisäksi periaatepäätöksessä Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (10.6.2021) yhdeksi toimenpiteeksi on kirjattu uusien toimintatapojen etsiminen tietoturvauhkista ja -loukkauksista viestimiseksi ja ilmoittamiseksi. Tehtävä on vastuutettu Liikenne- ja viestintävirastolle.

Jatkoseurannan perusteella tilannekuvan luontiin liittyvän ohjeistuksen voidaan katsoa parantuneen etenkin vakavien tietoturvapoikkeamien osalta, kun kyseessä on valtion yhteinen tukipalvelu. Tätä voidaan pitää myönteisenä ja tarkastuksessa esitetyn suosituksen suuntaisena. Vaikka poikkeamailmoitusten teko on yleistynyt, tarkastusvirasto katsoo, että ilmoitusten tekemiseen pitäisi yhä kannustaa. Ilmoittamatta jättämisen ei nähdä olevan kenenkään edun mukaista pidemmällä aikavälillä. Selvityksestä ei käy ilmi, että tarkastusviraston suositteleman ilmoitusvelvoitteen kustannuksista ja hyödyistä olisi tehty vaikutusarviointia.

Jatkoseurannassa saadun selvityksen perusteella voidaan todeta, että ilmoituskäytännöt ovat parantuneet tarkastuksen jälkeen.

3 Yhteenveto ja jatkotoimet

Tarkastuksen suositukset koskivat operatiivisen hallinta- ja johtamismallin kehittämistä valtionhallinnon ICT-palvelujen laajavaikutteisiin kyberhäiriötilanteisiin, palveluiden kybersuojauksen rahoitusta koko niiden elinkaaren ajan ja kyberloukkausten ilmoittamista Kyberturvallisuuskeskukselle. Tarkastuksen suositukset kohdistuivat valtiovarainministeriöön. Myös valtionhallinnon kyberturvallisuuden vahvistamiseen erityisesti osoitetut valtion talousarvion määrärahat on budjetoitu valtiovarainministeriölle.

Jatkoseurannan perusteella voidaan todeta, että tarkastuksen suositukset ovat toteutuneet osittain ja suositusten mukaisia toimia on monin osin käynnissä. Valtiovarainministeriö on kybersuojauksen järjestämisessä pyrkinyt siihen, että lausuntomenettely tukisi kybersuojauksen huomiointia osana palveluiden elinkaaren rahoitusta. Lausuntomenettelyn todellinen vaikuttavuus jää jatkoseurannan perusteella epäselväksi. Varmistaakseen kyberloukkauksista tehtävien häiriöilmoitusten paremman kattavuuden,

valtiovarainministeriön JulkICT-osasto on syksyllä 2021 antanut palveluntuottajille ohjeistuksen aiheesta. Kyberturvallisuuskeskuksen ja valtionhallinnon välisen tiedonvaihdon kuvataan lisäksi parantuneen viime vuosien aikana. Laajavaikutteisten kyberhäiriötilanteiden operatiivisen johtamisen vastuiden ja järjestelyjen määrittelyyn on perustettu koordinaatioryhmä. Tässä vaiheessa ei kuitenkaan vielä varmuudella voida sanoa, miten ryhmän tavoitteeksi kaavailtu selvitysraportti vastaa tarkastusviraston suositukseen.

Edellä kuvatun perusteella valtiovarainministeriö on alkanut kehittää kybersuojauksen järjestämistä tarkastuksessa esitettyjen suositusten suuntaan. Ministeriön kannattaa kiinnittää huomiota siihen, miten käynnissä olevat toimet vastaavat annettuihin suosituksiin.

Jatkoseurannan perusteella jälkiseurantaa ei ole tarvetta jatkaa. Kybersuojauksen järjestämiseen liittyviä asioita seurataan kuitenkin tarkastusviraston vuotuisessa suunnitteluprosessissa. Tarkastusvirasto on käynnistämässä vanhoihin tietojärjestelmiin kohdistuvan tarkastuksen kevään 2022 aikana. Tässä tarkastuksessa käsitellään mahdollisesti myös kybersuojausta ja tietoturvallisuutta järjestelmien elinkaarenhallinnan ja korjausvelan näkökulmasta.

Jaakko Eskola
johtaja, Toimiva tiedonhallinta

Sonja Huotari
projektiasiantuntija

JAKELU valtiovarainministeriö
TIEDOKSI liikenne- ja viestintäministeriö