

Jakelussa mainitut

Tarkastuskertomus 16/2017 Kybersuojauksen järjestäminen

Jälkiseurantaraportti

Valtiontalouden tarkastusvirasto on tehnyt jälkiseurannan viitekohdassa mainitusta tarkastuksesta.

Jälkiseurantaraportissa selvitetään, miten tarkastuksen kohteena oleva asia on kehittynyt, ja mihin toimiin tarkastuskertomuksessa annettujen suositusten ja kannanottojen johdosta on ryhdytty. Raportin tietoja hyödynnetään raportoitaessa vuosittain eduskunnalle olennaisista tarkastushavainnoista sekä viraston tarkastustoiminnan kohdentamisessa.

1 Jälkiseurannan toteutus

Jälkiseurannassa selvitettiin, miten viitekohdassa mainitussa tarkastuksessa annetut suositukset ovat toteutuneet. Suositukset perustuivat Valtiontalouden tarkastusviraston tarkastuksessaan tekemiin keskeisiin havaintoihin ja johtopäätöksiin siitä, oliko valtionhallinnon kybersuojaus tarkastuksen toteuttamishetkellä järjestetty mahdollisimman vaikuttavasti ja taloudellisesti tarkoituksenmukaisella tavalla. Tarkastusvirasto suositteli, että

1. valtiovarainministeriö määrittelee ja toteuttaa valtionhallinnon ICT-palveluiden osalta laajavaikutteisten kyberhäiriötilanteiden operatiivisen hallinta- ja johtamismallin
2. valtiovarainministeriö selvittää, miten palveluiden kybersuojaus tulisi ottaa huomioon palveluiden koko elinkaaren rahoituksessa
3. valtion tieto- ja viestintätekniikkakeskus Valtori (jäljempänä Valtori) parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä
4. valtiovarainministeriö parantaa kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle.

Tarkastuksen kohteena olevasta asiasta vastaavia viranomaisia ovat valtiovarainministeriön ja Valtorin lisäksi valtioneuvoston kanslia, liikenne- ja viestintäministeriö, valtionhallinnon keskitettyjä palveluja hoitavat viranomaiset, oman kybersuojauksensa järjestämisen osalta kaikki muutkin valtion viranomaiset sekä kyberturvallisuutta edistävät ja ylläpitävät tahot muuallakin kuin julkisella sektorilla.

Jälkiseuranta toteutettiin suunnitelman mukaisesti. Valtiovarainministeriölle ja Valtorille lähetettiin 4.11.2019 selvityspyyntö suositusten toimeenpanosta. Valtiovarainministeriö antoi selvityksensä 28.11.2019, minkä jälkeen ministeriön kanssa keskusteltiin 12.12.2019 sekä selvityksestä että mm. talousarvion määrärahojen käytöstä kyberturvallisuuteen. Lisäksi jälkiseurannassa perehdyttiin mm. valtioneuvoston periaatepäätöksenä antamaan Suomen kyberturvallisuusstrategiaan (3.10.2019) ja sen tausta-aineistoon, valtiovarainministeriön ja Valtorin välisiin tulossopimuksiin sekä valtiovarainministeriön kannanottoihin Valtorin tilinpäätöksistä viime vuosilta.

2 Jälkiseurannan havainnot

Operatiivinen hallinta- ja johtamismalli valtionhallinnon ICT-palvelujen laajavaikutteisiin kyberhäiriötilanteisiin

Valtiovarainministeriö ei ole uudistanut valtionhallinnon ICT-palvelujen operatiivista hallinta- ja johtamismallia. Valtiovarainministeriö kuvaa selvityksessään valtioneuvoston ohjesäännön mukaista toimintaa laajavaikutteisessa kyberhäiriötilanteessa ja mm. vuonna 2014 aloitettuja kehittämishankkeitaan. Kuvaukset eivät muuta käsitystä, joka Valtiontalouden tarkastusvirastolle muodostui kybersuojausta koskevassa tarkastuksessa ja jonka perusteella tarkastusvirasto suositteli, että valtiovarainministeriön kehittää operatiivisen hallinta- ja johtamismallin valtionhallinnon ICT-palvelujen laajavaikutteisiin kyberhäiriötilanteisiin.

Tarkastuksen jälkeen muualla valtionhallinnossa on kehitetty malli, joka vahvistaa ICT-palvelujen hallintaa laajavaikutteisissa kyberhäiriötilanteissa. Sen voidaan odottaa vaikuttavan myös operatiivisella tasolla. Suomen kyberturvallisuusstrategian 2019 (4.10.2019) mukaisesti kyberturvallisuuden kansallisen kehittämisen koordinoimiseksi liikenne- ja viestintäministeriöön on perustettu kyberturvallisuusjohtajan tehtävä. Kyberturvallisuusjohtaja koordinoi kyberturvallisuuden kehittämistä, suunnittelua ja varautumista, ja hänen johdolla laaditaan mm. kyberturvallisuuden kokonaiskuva ja kehittämisohjelma. Mallia kuvataan valtioneuvoston selvitys- ja tutkimustoiminnan tutkimuksessa ”Kyberturvallisuuden strateginen johtaminen Suomessa” (VN-TEAS 28/2018, 29.3.2018). Kuvauksen perusteella malli edistää tarkastusviraston antamien kybersuojausta koskevien suositusten toteutumista eri tavoin.

Palveluiden kybersuojauksen koko elinkaaren kattava rahoitus

Valtiovarainministeriön selvityksestä ei käy ilmi, mitä toimenpiteitä ministeriö on toteuttanut palveluiden koko elinkaaren kattavan kybersuojauksen rahoitukseen liittyen ja millä tavalla toimenpiteet muuttavat tarkastuksen aikaista tilannetta. Ainoana rahoitukseen liittyvänä asiana ministeriö mainitsee budjettiteknisen muutoksen, joka koskee Kyberturvallisuuskeskuksen tilannekuvan tuottamiseen liittyvän nk. GovCERT-palvelun rahoitusta. Selvityksestä käydyssä keskustelussa ministeriö katsoi, ettei se näe tarvetta muuttaa budjetointimenettelyjä suosituksen johdosta.

Edellä kerrotun lisäksi valtiovarainministeriö selvityksessään myös

- viittaa tarkemmin yksilöimättömiin ohjeisiin ja linjauksiin, jotka korostavat kybersuojauksen huomiointia osana palveluita ja toimintaa
- kertoo selvittävänsä kybersuojauksen kustannuksia erillisillä selvityksillä ja ottavansa kybersuojauksen huomioon hankearviointissa, hallinnonalayhteistyössä ja hallinnonalojen budjettiesityksiin tehtävissä JulkICT:n kannanotoissa
- kuvaa Väestörekisterikeskuksen, Kyberturvallisuuskeskuksen ja Keskusrikospoliisin toimintaa kybersuojauksessa mainiten esimerkiksi, että Väestörekisterikeskus muodostaa kyberturvallisuuden strategisen tason tilannekuvan.

Tarkastusvirasto pyrki suosituksellaan edistämään sitä, että valtion talousarvion määrärahat kohdistuisivat kybersuojauksen kokonaisuuden kannalta tärkeimpiin kohteisiin ja turvaisivat Kyberturvallisuuskeskuksen toimintaedellytykset. Valtion talousarvioesityksessä vuodelle 2020 on määrärahalisäyksiä kyberturvallisuuden vahvistamisen kannalta keskeisille valtion viranomaisille. Tämä on Suomen kyberturvallisuusstrategian 2019 mukaista: kriittisistä toiminnoista vastaavien viranomaisten kyberturvallisuuden ohjaus-, tuki- ja valvontavastuita sekä näiden edellyttämiä resursseja ja keinovalikoimaa parannetaan kaikilla hallinnon aloilla ja tasoilla.

Valtioneuvoston ohjesäännön (262/2003) 17. §:n perusteella valtiovarainministeriön toimialaan kuuluvat valtionhallinnon tietohallinnon ohjaus, sähköisen asioinnin ja tietoturvallisuuden yleiset perusteet sekä valtion ja kuntien tietohallintoyhteistyö. Määrärahat erityisesti valtion ICT:n ohjausta ja

kehittämistä varten on budjetoitu valtion talousarviossa valtiovarainministeriön pääluokkaan, momentille 28.70.01. Momentin määrärahat vuosilta 2014–2019 ovat yhteensä yli 34 miljoonaa euroa. Ministeriön seurantatiedoista ei ilmene, paljonko määrärahasta on tosiasiallisesti käytetty kybersuojaukseen. Valtiovarainministeriö on osoittanut osan määrärahasta valtion muille viranomaisille.

Kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutuksen, arvioinnin ja kehittämisen parantaminen Valtorissa

Valtori on antamansa selvityksen perusteella toteuttanut suositusta asianmukaisesti. Selvityksessä kuvataan kattavasti toimenpiteitä, joilla virasto on kehittänyt kybersuojauksen menettelyjä sekä kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä. Selvitys on salassa pidettävä.

Valtiovarainministeriön vuotta 2018 koskevan tilinpäätöskannanoton mukaan asiakkaiden toiminnan jatkuvuuden varmistaminen on ollut Valtorin kanssa tehdyn tulossopimuksen tärkein tavoite. Ministeriön arvio tavoitteen saavuttamisesta vuonna 2018 laski edellisvuodesta. Kannanotossaan ministeriö pitää jatkuvuuden kannalta kyberuhkiin varautumista entistä tärkeämpänä. Ministeriö on antamansa selvityksen perusteella varmistanut Valtorin kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin, arvioinnin ja kehittämisen parantamista keinoilla, joita ministeriöt yleensäkin käyttävät toimialansa ohjauksessa. Niihin kuuluu mm. tulosohejaus. Ministeriön ja Valtorin välisissä tulossopimuksissa vuosille 2017–2019 on kyberturvallisuutta koskevia tavoitteita.

Kyberloukkausten ilmoittaminen Kyberturvallisuuskeskukselle

Valtiovarainministeriö ei ole nähnyt perusteita sille, että kyberloukkausilmoituksista ilmoittaminen Kyberturvallisuuskeskukseen tehtäisiin tarkastusviraston antaman suosituksen mukaisesti nykyistä velvoittavamaksi. Kyberloukkauksien ilmoittamisesta on jo olemassa suositus, johon ministeriö viittaa selvityksessään. Suositus sisältyy helmikuulle 2017 päivättyyn Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeeseen ”Tietoturvapoiikkeamatilanteiden hallinta”. Suositus ei ole velvoittava.

Lakiin perustuva kyberloukkausten ilmoittamisvelvollisuus on ministeriön mukaan sääteilyllisesti ylimitoitettu ja hallinnollisesti raskas. Ilmoitusvelvoitteesta ei ole tehty vaikutusarviointia, joka ottaisi huomioon mm. ilmoittamisesta johtuvat kustannukset ja hyödyt. Edelleen, lakimuutos vaatisi Kyberturvallisuuskeskuksen roolin, ilmoittajien vastuiden, toimivaltuuksien ja toimenpiteiden ohjauksen uudelleen tarkastelua. Ministeriö on kuitenkin valmis tarkistamaan kantaansa ilmoitusvelvollisuuteen, jos osoitetaan, että nykyiset järjestelyt eivät riitä. Tarkastusvirasto pyrki kyberloukkauksien ilmoittamista koskevalla suosituksella edistämään viranomaisten kykyä parantaa kyberuhkien havainnointimahdollisuuksia. Kyberturvallisuuskeskus arvioi, että ilmoituksia ei tule riittävän laajasti.

3 Yhteenveto ja jatkotoimet

Valtiovarainministeriö ei ole ryhtynyt riittäviin toimenpiteisiin kolmen suosituksen johdosta, jotka Valtiontalouden tarkastusvirasto esitti sille tuloksellisuustarkastuskertomuksessa 16/2017 Kybersuojauksen järjestäminen. Suositukset koskivat operatiivisen hallinta- ja johtamismallin kehittämistä valtionhallinnon ICT-palvelujen laajavaikutteisiin kyberhäiriötilanteisiin, palveluiden kybersuojauksen rahoitusta koko niiden elinkaaren ajan ja kyberloukkausten ilmoittamista Kyberturvallisuuskeskukselle. Ministeriö on suositusten toimeenpanossa toimivaltainen viranomainen. Myös valtionhallinnon kyberturvallisuuden vahvistamiseen erityisesti osoitetut valtion talousarvion määrärahat on budjetoitu valtiovarainministeriölle.

Suomessa on kuitenkin vahvistettu kybersuojausta myös muiden viranomaisten kuin valtiovarainministeriön toimenpitein. Meneillään on kyberturvallisuuden strategisen johtamisen muutos kyberturvallisuusjohtaja-mallin mukaiseksi. Valtion talousarvioesityksessä vuodelle 2020 määrärahoja on lisätty kyberturvallisuuden vahvistamisen kannalta keskeisille valtion viranomaisille, kuten valtioneuvostolle,

liikenne- ja viestintäministeriölle sekä Liikenne- ja viestintävirastoon (Traficom) sijoitetulle Kyberturvallisuuskeskukselle. Toimenpiteet edistävät operatiivisen hallinta- ja johtamismallin kehittämistä valtionhallinnon ICT-palvelujen laajavaikutteisiin kyberhäiriötilanteisiin ja muutoinkin suositusten toteuttamista. Lisäksi Valtorissa on meneillään tarkastusviraston suosituksen mukaisia toimenpiteitä.

Edellä esitetyn perusteella jälkiseuranta on tarpeen jatkaa edellä mainitun kolmen toteuttamatta olevan suosituksen osalta (operatiivinen hallinta- ja johtamismalli laajavaikutteisiin kyberhäiriötilanteisiin, kybersuojauksen rahoitus ja kyberloukkausilmoitukset Kyberturvallisuuskeskukselle). Toisaalta kokonaan uutta tarkastusta aihealueelta puoltaisivat kybersuojauksen järjestelyissä ja digitaalisessa toimintaympäristössä meneillään olevat muutokset riskeineen sekä kyberturvallisuuden valtiontaloudellinen ja muu merkitys tietoyhteiskunnassa.

Jaakko Eskola
johtaja, Toimiva tiedonhallinta

Matti Mattila
tuloksellisuustarkastusneuvos

JAKELU Valtiovarainministeriö
Valtion tieto- ja viestintätekniikkakeskus Valtori