Tuija Kuusisto, tietohallintoneuvos
Niko Mäkilä, neuvotteleva virkamies
Valtiovarainministeriö
2.3.2026

Viite: Eduskunnan hallintovaliokunta; keskiviikko 04.03.2026 klo 11.15

Asia: VNS 6/2025 vp Valtioneuvoston selonteko sisäisestä turvallisuudesta

Kyberturvallisuutta vakavasti vaarantavien tilanteiden havaitsemisesta ja torjumisesta

Valtiovarainministeriö kiittää mahdollisuudesta tulla kuulluksi liittyen Valtioneuvoston selontekoon sisäisestä turvallisuudesta (VNS 6/2025). Valtiovarainministeriötä on pyydetty lausunnossaan keskittymään seuraaviin kahteen kysymykseen, joihin liittyviä näkökulmia on käsitelty tässä asiakirjassa.

Mitkä ovat keskeisimmät lainsäädännön muutostarpeet kyberuhkien havaitsemiseen ja torjuntaan liittyvien tavoitteiden toteuttamiseksi?

Kyberuhkien havaitsemisessa ja torjumisessa avainasemassa ovat viranomaisten tietojärjestelmien ja digipalveluiden tietoturvallisuuden riskiperustainen, koko elinkaaren ajan toteutettava tietoturvallisuuden ja varautumisen vaatimusten toteutumisen tekninen arviointi sekä tietojärjestelmien ja digipalveluiden poikkeamien havainnointi ja niihin reagointi eli jatkuva tekninen seuranta. Teknisen arvioinnin ja seurannan tulee perustua ajantasaiseen tietoon kyberuhkista ja -riskeistä.

Turvallisuusympäristön muutokset ovat kasvattaneet tarvetta nostaa viranomaisten tietojärjestelmien ja digipalveluiden turvallisuuden tasoa. Tämä on lisännyt tietojärjestelmien tietoturvallisuuden arviointipalvelujen kysyntää. Valtiovarainministeriössä on valmisteltu hallituksen esitys eduskunnalle laeiksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain ja tietoturvallisuuden arviointilaitoksista annetun lain muuttamisesta. Esitys on suunniteltu annettavaksi kevään 2026 istuntokaudella.

Ehdotuksella vastataan arviointitarpeiden kasvuun. Tavoitteena on parantaa arviointien saatavuutta, sujuvoittaa arviointimenettelyä, selkeyttää arviointiperusteita sekä tehostaa viranomaisyhteistyötä. Tavoitteena on, että viranomaiset hyödyntäisivät tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuus- ja varautumistoimenpiteiden mitoittamisessa tilanteeseen soveltuvaa arviointimenettelyä turvallisuuden edistämiseksi.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettuun lakiin ehdotetuilla muutoksilla

laajennettaisiin arviointi varautumisen arviointiin sekä turvallisuuskriittisten tuotteiden arviointiin. Turvallisuuskriittiset tuotteet liittyvät muun muassa tiedon ja tietoliikenteen salaukseen ja tietojärjestelmien hajasäteilysuojaukseen. Arviointiviranomaisina toimisivat nykyisen Liikenne- ja viestintäviraston lisäksi Pääesikunnan määrätty turvallisuusviranomainen, joka voisi arvioida Puolustusvoimien tietojärjestelmiä. Valtionhallinnon viranomaisille säädettäisiin velvollisuus arvioida tietojärjestelmänsä ja tietoliikennejärjestelynsä vähintään itsearviointeina. Lakiin täydennettäisiin uudeksi arviointimenettelyksi myös viranomaisen toimeksiannosta toteutettu arviointi, ja luotettaviksi todetuille yrityksille säädettäisiin mahdollisuus tarjota tietoturvallisuuden ja varautumisen arviointipalveluja viranomaisille korkeintaan turvallisuusluokan IV tietojen käsittelyn arviointiin saakka.

Kaikkien soveltamisalaan kuuluvien viranomaisten tulisi pyytää arviointiviranomaisen arviointia turvallisuusluokan I ja II tietojen käsittelylle. Viranomaisten tulisi pyytää arviointiviranomaisen arviointia tai hankkia tietoturvallisuuden arviointilaitoksen arviointi myös turvallisuusluokan III tietojen käsittelylle, ellei viranomainen riskiarvioinnin perusteella päättäisi sen olevan tarpeetonta. Viranomaisten lisäksi turvallisuuskriittisten tuotteiden valmistajille säädettäisiin oikeus hakea tuotteensa arviointia.

Ehdotetuilla muutoksilla tehostettaisiin arviointeja korostamalla riskiarvion merkitystä arviointimenettelyn valinnassa ja painotettaisiin viranomaisten vastuuta omien tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuudesta ja varautumisesta sekä käyttöönottopäätöksistä. Muutoksilla myös tarkennettaisiin ja tehostettaisiin arviointiviranomaisten yhteistyötä, työjakoa ja tiedonsaantioikeuksia sekä mahdollistettaisiin arviointiviranomaista avustava tehtävä.

Tietoturvallisuuden arviointilaitoksista annettuun lakiin ehdotetuilla muutoksilla edistettäisiin tietoturvallisuuden arviointilaitosten elinkeinotoiminnan edellytyksiä yksinkertaistamalla ja tehostamalla tietoturvallisuuden arviointilaitosten luotettavuuden sääntelyä ja joustavoittamalla tietoturvallisuuden arviointilaitosten pätevyyksien hyväksyntää.

Millä lainsäädännöllisillä toimenpiteillä voidaan vaikuttaa siihen, että esim. Valtorin tietomurron kaltaiset teot voidaan jatkossa nykyistä tehokkaammin estää ja teoista aiheutuvat vahingot minimoida?

Valtiovarainministeriössä on ollut 1.10.2024 lähtien käynnissä Tori- ja Tuve-toiminnan kehittämishanke (T2-hanke), jossa toteutetaan valtion yhteisten

tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013) ja julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015) nykytilan arviointi, tavoitetilan määrittely sekä tunnistetaan lainsäädännön ja muut kehitystarpeet. Hankkeen tavoitteena on parantaa valtion yhteisten tieto- ja viestintäteknisten palvelujen sekä palvelutuotannon kustannustehokkuutta ja tuottavuutta, selkeyttää valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämistä ja siihen liittyviä tehtäviä sekä vastuita sekä mahdollistaa palveluissa tehokas uusien teknologioiden hyödyntäminen ja kyvykkyyksien kehittäminen ja huomioida nykyistä kattavammin ja yhtenäisesti vaatimukset valtion yhteisten tieto- ja viestintäteknisten palvelujen yhteentoimivuudesta, turvallisuudesta ja varautumisesta. Hankkeen aikana tarkastellaan myös mahdolliset säädösmuutostarpeet koskien yhteisten tieto- ja viestintäteknisten palvelujen tietoturvallisuuden ja varautumisen yhteisesti toteutettua arviointia. Hankkeen määräaika on 30.6.2027, minkä jälkeen on tarkoitus tarvittaessa aloittaa valtion yhteisiin tieto- ja viestintäteknisiin palveluihin liittyvä säädösvalmistelu.

Valtiovarainministeriön vastuulla on julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jatkossa tiedonhallintalain) valmistelu. Valtiovarainministeriössä suunnitteilla on ollut aloittaa tiedonhallintalain jälkiarviointityö, mutta arvioinnin aloittamisajankohtaa ei ole kiinnitetty. Tiedonhallintalain jälkiarviointityön yhteydessä on tarkoituksenmukaista tarkastella myös laissa säädettyjen tietoturvallisuuden vähimmäisvaatimusten sekä turvallisuusluokitteluvelvoitteen soveltamisalan ajantasaisuutta.

Kyberturvallisuuden turvallisuusluokiteltua tilanne- ja ennakointitietoa ei ole kattavasti jaettu kaikille julkisen hallinnon toimijoille kuten hyvinvointialueille ja kuntiin, koska tiedonhallintalaissa säädetty turvallisuusluokitteluvelvoite ja siten säännökset turvallisuusluokiteltujen tietojen käsittelystä eivät koske kaikkia julkisen hallinnon toimijoita. Tämä on hankaloittanut toimintaa häiriötilanteissa ja kriiseissä. Valtiovarainministeriössä on käynnistetty turvallisuusluokitteluvelvoitteen mahdollisen laajentamisen esiselvitys, jossa arvioidaan laajentamisen tarvetta ja kustannuksia. Velvoitteiden laajentamisen esimerkiksi kuntiin ja hyvinvointialueisiin on arvioitu olevan merkittävä lisäkustannuskysymys.

EU:n NIS2-kyberturvallisuusdirektiivissä osoitetaan yhteiskunnan kriittisille sektoreille kyberturvallisuutta vahvistavia riskienhallintavelvollisuuksia sekä merkittäviä poikkeamia koskevia raportointivelvollisuuksia. NIS2-direktiivin

kansallinen toimeenpano vuonna 2025 sekä siihen liittynyt uuden kyberturvallisuuslain (124/2025) voimaantulo ja direktiivin julkinen hallinto -toimialan osalta tiedonhallintalakiin lisättyjen säännösten voimaantulo laajensi ja yhdenmukaisti yhteiskunnan turvallisuusvaatimuksia. Kaikki julkisen hallinnon toimijat eivät kuitenkaan sisälly kyberturvallisuuslaissa ja laissa julkisen hallinnon tiedonhallinnasta säädettyjen kyberturvallisuusvaatimusten soveltamisalaan. NIS2-kyberturvallisuusvelvoitteiden laajentamisen koko kuntakentälle arvioitiin olevan merkittävä kustannuskysymys ja siksi kuntakentällä ei ole esimerkiksi yleistä velvoitetta tietojärjestelmien ja digipalvelujen poikkeamien havainnointiin ja niihin reagointiin.

EU:n kyberkestävyyssäädös (EU 2024/284) koskee digitaalisen elementin sisältäviä laitteita tai ohjelmistoja, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Säädöksen mukaisia tietoturvaominaisuuksia koskevia vaatimuksia sovelletaan kuitenkin vasta 11.12.2027 alkaen eli 36 kuukauden siirtymällä säädöksen voimaantulosta. Näitä vaatimuksia ovat muun muassa turvalliset oletusasetukset ja automaattiset turvallisuuspäivitykset, luvattomalta pääsyltä estäminen sekä datan luottamuksellinen säilyttäminen ja datan minimointi. Vaatimukset koskevat myös julkisen hallinnon käyttämiä digitaalisen elementin sisältämiä laite- ja ohjelmistotuotteita.

Valtion tieto- ja viestintätekniikkakeskus Valtorin 3.2.2026 julkaisemassa tiedotteessa koskien mobiililaitteiden hallintapalvelussa tapahtunutta tietomurtoa todettiin muun muassa seuraavaa: ”Hyökkääjä hyödynsi Valtorin käyttämän valmisohjelmiston haavoittuvuutta, johon ei sen julkaisuhetkellä 29.1. ollut saatavilla korjaavaa päivitystä. Valtori teki korjauksen välittömästi torstai-iltapäivän 29.1. aikana korjauspäivityksen julkaisun jälkeen sekä myöhemmin esti hyökkääjän toiminnan eristämällä mobiilihallintapalvelun verkosta.” Tämä Valtorin palveluun kohdistunut tietomurto on esimerkki siitä, että käytännössä kaikki avoimessa verkossa olevat tietojärjestelmät on mahdollista murtaa, eikä tätä ole mahdollista lainsäädännöllä täysin estää.

Valtori kertoi 3.2.2026 julkaistussa tiedotteessa myös tiedottaneensa tilanteesta tietoturvapoikkeamien hallintaprosessin mukaisesti asiakasorganisaatioidensa tietoturva- ja muita avainyhteyshenkilöitä, sekä tehneensä rikosilmoituksen ja jatkavansa tilanteen tutkintaa viranomaisyhteistyössä poliisin ja Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen kanssa. Kyseisen tietomurron tapauksessa Kyberturvallisuuskeskuksen tietoturvaloukkausten käsittelyprosessi sekä

turvallisuusviranomaisten asiaan liittyvät prosessit ovat siten toteutuneet hyvin.

Valtiovarainministeriössä on perehdytty tarkasti Valtorin palvelun tietomurron tapahtumiin ja vaikutuksiin, ja tarkoituksena on hyödyntää tietomurrossa saatua kokemusta sekä lainsäädännöllisissä toimenpiteissä, että kyberturvallisuuden ohjeistuksen, prosessien, menetelmien ja käytänteiden edistämisessä julkisessa hallinnossa.