3.10.2022

22-2168

Max Hamberg

Asiantuntijalausunto eduskunnan valtiovarainvaliokunnalle

Valtioneuvoston ja sen ministeriöiden kyberturvallisuutta on kehitetty määrätietoisesti useiden vuosien ajan. Valtioneuvoston kanslia toimialaan kuuluu valtioneuvoston ja sen ministeriöiden sekä Suomen ulkomaanedustustojen tieto- ja viestintätekniset peruspalvelut, asiakirjahallinto ja valtioneuvoston turvallisuus ja varautuminen. Valtioneuvoston kanslia toimii ministeriöiden lukuun asiakirjahallinnon tehtävissä ja hyvän tiedonhallintatavan edellyttämissä toimenpiteissä, mukaan lukien Euroopan unionia ja kansainvälisiä asioita koskeva tiedonhallinta.

Suomen ja Euroopan turvallisuus- ja toimintaympäristössä on tapahtunut perustavanlaatuinen muutos Venäjän hyökättyä Ukrainaan. Ulko- ja turvallisuuspoliittisen toimintaympäristön muuttuminen heijastuu myös kyberympäristössä. Kyberhyökkäykset ovat osa Venäjän hyökkäystä Ukrainaan. Venäjä todennäköisesti laajentaa kyber- ja informaatio-operaatioitaan Ukrainasta länteen. Tilanne on kehittynyt kevään jälkeen huolestuttavaan suuntaan.

Monilla valtioilla sekä muilla toimijoilla on hallussaan kybersuorituskykyjä, joiden avulla voidaan häiritä, vahingoittaa tai hyväksikäyttää toisen osapuolen tietojärjestelmiä. Kyberympäristön uhat ovat monimutkaistuneet ja lisääntyneet erityisesti yhteiskunnan eri toimijoiden digitalisaatiosta johtuen.

Suomalainen kyberturvallisuus ja -puolustus vastatoimineen on mitoitettava torjumaan valtiollisen toimijan laaja-alainen kyberhyökkäys kansallista päätöksentekoa, turvallisuusviranomaistoimintaa ja kriittistä infrastruktuuria vastaan.

Valtioneuvoston kanslian tehtävänä on mahdollistaa hallituksen toiminta ja järjestää valtioneuvoston yleiset toimintaedellytykset. Valtion johtamisen on oltava mahdollista kaikissa turvallisuustiloissa. Valtioneuvoston työskentely on täysin riippuvaista toimivasta tietotekniikasta. Olennainen osa päätöksentekoa on tarkka ja oikea-aikainen tilannekuva; kaiken päätöksenteon tulee perustua tarkkoihin varmistettuihin faktoihin. Valmistelun ja päätöksenteon on oltava mahdollista ja yhteyksien eduskuntaan on toimittava kaikissa tilanteissa. Julkinen viestintä on keskeinen osa valtion johtamista ja myös sen merkitys korostuu turvallisuustilanteen kiristyessä. Kaikki tämä rakentuu nykypäivänä tietoteknisen toimintaympäristön toiminnan varaan.

Laajalti käytettyjen tietoteknisten ratkaisuiden turvallisuus voidaan rakentaa huomattavasti vahvemmaksi kuin monien erillisten ratkaisuiden turvallisuus. Tietoteknisten ratkaisuiden turvallisuuden varmistaminen aiheuttaa tyypillisesti korkeita kustannuksia, ja, jos ratkaisuita tehdään useita rinnakkain, kertautuvat näiden kustannukset. Yhteisiä palveluita tuottava toimija pystyy kehittämään osaamistaan ja ratkaisuita huomattavasti tehokkaammin kuin erilliset toimijat, joiden voi olla nykyisessä tilanteessa vaikeaa saada pelkästään rekrytoiduksi riittävää määrää kyberturvallisuuden osaajia tehtäviensä hoitamiseen. Tässä ei päde se, että kaikki munat pitäisi pitää eri koreissa, vaan se, että korit rakennetaan niin turvallisiksi, etteivät siellä olevat munat säry.

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Valtioneuvoston kanslia PL 23 00023 Valtioneuvosto	Snellmaninkatu 1 A Helsinki	0295 16001 +358 295 16001	09 1602 2165 +358 9 1602 2165	kirjaamo.vnk@gov.fi

Esimerkkinä yhteisten palveluiden turvallisuuden kehittämisestä on keväällä 2022 tehty laaja palvelunestohyökkäys, joka tapahtui samanaikaisesti, kun Ukrainan presidentti Volodymyr Zelenskyi piti puhettaan eduskunnalle. Yhdeksän yhteisessä julkaisujärjestelmässä olevan ministeriön sivulla ei hyökkäys aiheuttanut näkyvää häiriötä, koska yhteisen järjestelmän suojaukset oli voitu kehittää riittävän vahvoiksi. Kolmen erillisiin ympäristöihin jääneen ministeriön verkkosivut häiriytyivät näkyvästi. Julkisuudessa käsiteltiin tuolloin lähinnä vain niitä palveluita, joihin hyökkäys oli onnistunut. Onnistuneet hyökkäykset, vaikka eivät vakavia kaikki olisikaan, nousevat julkisuuskynnyksen yli ja ovat omiaan lisäämään huolta yhteiskunnassa.

Valtioneuvostossa tietoteknistä turvallisuutta rakennetaan kolmen vahvan korin periaatteella. Normaali valtioneuvostotyö tapahtuu turvallisessa normaalitasoisessa tietoteknisessä työympäristössä, joka mahdollistaa sujuvan ja joustavan yhteistoiminnan muun yhteiskunnan kanssa. Korkeampaa turvallisuutta varten on turvallisuusverkon (Tuve) palvelut, joita käytetään normaalien työvälineiden rinnalla niissä tehtävissä, joissa edellytetään korkeaa turvallisuutta tai varautumista. On tärkeää, että turvallisuusverkon palveluiden tietoturvallisuutta kehitetään siten, että myös ulko- ja puolustusministeriö ryhtyvät käyttämään niitä turvallisuusluokiteltujen aineistojensa käsittelyyn.

Näiden lisäksi valtioneuvostossa on ja tulee olemaan käytössään erillisratkaisuita korkeasti suojattavien aineistojen käsittelyyn. Nämä erillisratkaisut eivät ole avoimia julkisiin verkkoihin. Nato jäsenyyden myötä on ilmeinen tarve kehittää uusia erillisratkaisuita ja ratkaisut kannattaa kehittää siten, että niitä voidaan laajalti käyttää viranomaisten välisessä yhteistyössä, jolloin niihin tehtävät investoinnit vaikuttavat laajalti. Korkeammin turvallisuusluokiteltujen aineistojen oikea-aikainen toimittaminen edellyttää tällä hetkellä paperimenettelyihin tukeutuvien prosessien sähköistämistä.

Valtioneuvoston kanslia käyttää Valtion tieto- ja viestintätekniikkakeskus Valtorin tuottamia perustietoteknisiä palveluita. Näiden palveluiden tietoturvallisuutta on kehitetty viimeisten vuosien aikana merkittävästi valtioneuvoston kanslian ja Valtorin välisellä yhteistyöllä, ja kehitystyö jatkuu. Käynnissä on jatkuva kilpajuoksu ammattimaisten tai valtiollisten toimijoiden hyökkäyskyvykkyyksien ja puolustuskyvykkyyksien välillä. Tietoturvallisuusratkaisut eivät tästä syystä koskaan valmistu, vaan kehittämisen tulee olla jatkuvaa. Valtion yhteisten tietoteknisten palveluiden turvallisuuden kehittämiseen tuleekin kiinnittää riittävä jatkuva rahoitus.

Valtioneuvostossa ja sen ministeriöissä lisätään korkeamman tietoturvan ja korkeamman varautumisen palveluiden käyttöä jatkuvassa käytössä olevien peruspalveluiden rinnalla. Turvallisuusympäristön muutos lisää tarvetta kehittää myös viranomaiskohtaisia tietoturvapalveluita erityisesti havainnoinnin, valvonnan ja kapasiteetin riittävyyden osalta. Lisäksi palveluiden turvallisuuden varmistaminen edellyttää riittäviä henkilöstöresursseja sekä palvelun tuottajilla että viranomaisissa. Korkeimmin suojattavien aineistojen käsittely edellyttää hajasäteilysuojattuja järjestelmiä ja erityisiä käsittelytiloja, joissa hajasäteilysuojauksen lisäksi on tarvittavat turvallisuusjärjestelyt, mm. rikosilmoituslaitteet ja kameravalvonta. Sekä tietotekniikan että toimitilojen korkean turvallisuuden tason saavuttaminen ja korkeammin luokitellun tiedon käsittelyn tarpeen laajeneminen edellyttävät investointeja. Valtioneuvostossa nämä investoinnit on järkevintä toteuttaa kaikkien ministeriöiden osalta yhteiskäyttöisesti.

Käynnissä olevan kriisin myötä ja Suomen päästyä tarkkailijajäseneksi Natoon korkeammin luokiteltujen salassa pidettävien aineistojen määrä on jo kasvanut vuonna 2022 merkittävästi ja tulee kasvamaan entisestään. Korkeimmin luokitellut aineistot käsitellään ja jaellaan nykyisin pääasiassa paperilla, ja paperilla liikutettavan aineistomäärän kasvu on aiheuttanut välittömän henkilöstötarpeen. Suomen Nato jäsenyyden myötä tulee valtioneuvoston ja sen ministeriöiden toimintaa korkeimmin suojattujen aineistojen osalta kehittää sähköiseksi. Jäsenyys Natossa tulee vaikuttamaan ennen kaikkea ulko- ja puolustusministeriön toimintaan, mutta myös muihin ministeriöihin mm. resilienssityön ja yleisen kokonaisturvallisuuden ja varautumisen johdosta. Valtioneuvoston kanslian tehtävänä on järjestää ministeriöiden käyttöön tarvittavat ja riittävän turvalliset välineet ja ratkaisut.

Valtioneuvoston toimintavalmiuksia on tarkoitus kehittää ympärivuorokautisiksi. Kiireelliset ja myös korkeimmin luokitellut aineistot tulee pystyä toimittamaan turvallisesti vastaanottajille kaikkiin ministeriöihin kaikkina vuorokauden aikoina. Tämä edellyttää valtioneuvoston yhteistä rekisteri- ja jakelutoimintoa, josta voimassa olevien säädösten mukaan vastaa valtioneuvoston kanslia. Valtioneuvoston korkeimmin luokiteltavien aineistojen jakelu vaatii erityisesti kansainvälisten erityissuojattavien aineistojen osalta tiukkaa todennettua tietoturvan tasoa, henkilöstövoimavaroja sekä tietoteknisiä ja tilaturvallisuuteen liittyviä investointeja.

Viestintäratkaisuiden, sähköpostiratkaisun ja videoneuvotteluratkaisuiden tulee sekä kotimaassa että Suomen ulkomaan edustustoissa olla turvallisia ja yhteyksien reaaliaikaisia. Valtioneuvoston käytössä olevien tietoteknisten palveluiden turvallisuutta tulee jatkuvasti kehittää sekä valvoa samoin kuin varautua ympärivuorokautisesti mahdollisiin hyökkäys- ja häiriötilanteisiin. Tätäkään kyvykkyyttä ei ole taloudellista rakentaa laajalti erillisiin viranomaisiin.

Valtioneuvoston jatkuvassa käytössä olevien tietoteknisten palveluiden turvallisuus varmistetaan jatkuvalla kehittämisellä. Lisäksi tarvitaan erillisiä turvallisuusjärjestelmiä. Korkeammin suojattavien aineistojen sähköinen käsittely edellyttää teknisiä rekisteri- ja jakeluratkaisuja, joissa on hyväksytyn arviointilaitoksen todentama tietoturvataso. Lisäksi valtionjohdon oikea-aikaisen tilannekuvan muodostaminen edellyttää uutta verkottunutta tilannekuvajärjestelmää. Valtioneuvostolle ja valtiojohdolle tulee voida tuottaa ja esittää turvallisuustilanteen hallinnan vaatima tilannekuva tietoturvallisuuden vaatimukset täyttäen. Tietomäärän kasvun myötä ja tiedon eheyden säilyttämiseksi tilannekuvajärjestelmää on kehitettävä sekä valtioneuvoston tilannekeskuksen ja hallinnonalojen välisten järjestelmien integraatiota on parannettava.

Myös tietoturvallisuuden hallintaa ja johtamista tulee kehittää jatkuvasti. Toiminnan jatkuvuuden varmistamiseksi tulee kehittää johdonmukaisesti tietojärjestelmien palautumissuunnittelua mutta myöskin organisaatioiden kykyä jatkaa toimintaa häiriöistä huolimatta. Organisaatioiden jatkuvuussuunnittelulle on varmistettava riittävä resursointi. Turvallisuusympäristön muuttuessa valtioneuvoston koko henkilöstön tietous ja valmius ymmärtää, havaita ja raportoida tietoturvauhkia ja mahdollisia tietoturvatapahtumia tulee olla ajan tasalla. Tämä vaatii laaja-alaista investointia myös koko henkilöstön osaamiseen.

Talouden näkökulmasta on olennaisen tärkeää, että valtionhallinnon tasolla varmistetaan valtion tieto- ja viestintätekniikkakeskuksen tuottamien palveluiden riittävä tietoturvallisuuden ja varautumisen taso. Valtioneuvoston kanslian näkökulmasta on varmistettava lisäksi riittävät voimavarat ja rahoitus jatkuvassa käytössä olevien tietoteknisten palveluiden sekä asiakirjahallinnon turvallisuuden sekä valtion johdon tilannekuvan jatkuvaksi kehittämiseksi. Ukrainan sodan ja tulevan Nato-jäsenyyden myötä yhä aikakriittisemmäksi muuttuvassa toiminnassa nähdään erityisen tärkeäksi kansainvälisten aineistojen käsittelyyn tarvittavien toiminnallisten ja teknisten ratkaisuiden rakentaminen valtioneuvoston käyttöön.

Liitteet Napsauta tähän hiirellä ja kirjoita liitteiden nimet kukin omalle rivilleen. Rivinvaihto enterillä.

Jakelu

Tiedoksi