Ulkoministeriö
Hallintopalvelut
Tietohallintojohtaja Ari Uusikartano

Eduskunnan tarkastusvaliokunnalle 27.9.2022

Asia: K 2/2021 vp Hallituksen vuosikertomus 2021

Aihe: Seuraava kannanotto (Hallituksen vuosikertomus 2021, liite 3, s. 81) UM:n tietoturvajärjestelyt (EK 25/2019 – K 3/2019 vp – K 13/2019 vp)
”5. Eduskunta edellyttää, että hallitus jatkaa toimenpiteitä ulkoasiainhallinnon tietoturvajärjestelyjen parantamiseksi ja raportoi niistä hallituksen vuosikertomuksessa.”

Yleistä

Ulkoministeriön tieto- ja kyberturvallisuuskyvykkyyksiä on kehitetty vuosien ajan systemaattisesti. Ministeriön tietoturvallisuustoiminta on ollut sertifioitu ISO27001-standardin mukaiseksi vuodesta 2021 lähtien. Systematiikka on keskeinen apuväline tilanteessa, jossa hallinnonalaan kohdentuvat tieto-ja kyberturvallisuuteen liittyvät uhkatekijät ovat kasvaneet jatkuvasti. Hallinnonalan osalta tarkastelujaksolla 2021 – 2022 on tunnistettu toistuvasti kohdennettua tiedustelutoimintaa. Ilmiö on sinänsä ulkoasiainhallinnon näkökulmasta normaali, mutta toiminnan laatu on kehittynyt ja intensiteetti kasvanut. Ministeriö on tullut yhden vakavamman tapauksen osalta myös omatoimisesti julkisuuteen paljastettuaan diplomaatteihin kohdentunutta vakoilutoimintaa ns. Pegasus-vakoiluohjelman kautta.

Haasteena ministeriössä on koettu valtioneuvoston toiminnassa toteutetut tietotekniikka- ja järjestelmäpalvelujen keskittämistoimet, joiden seurauksena ministeriön aikaisemmin käyttämien dedikoitujen hallinta- ja valvontapalvelujen käyttömahdollisuudet ovat heikentyneet. Edelleen ulkoasiainhallinnon ollessa jatkuvan tiedustelutoiminnan kohteena, keskitetyt palvelut joihin hallinnonala tuodaan mukaan, vaarantavat välillisesti myös muiden ministeriöiden tiedonhallintaa sekä digitaalisen palveluympäristön toimintaa. Ulkoministeriön näkökulmasta tulisikin harkita, missä laajuudessa toteutettuna taloudellisuuden ja tuottavuuden parantamiseen tarkoitetut toimenpiteet kääntyvät itseään vastaan kokonaisuuden turvallisuuden vaarantuessa. Kaikkien toimintojen turvaamispyrkimysten toteuttaminen sille tasolle, mitä kriittisimmät niistä edellyttävät, ei myöskään ole taloudellisesti mahdollista ja toiminnallisesti tarpeellista.

Toimenpiteet osa-alueittain

Seuraavissa kappaleissa keskitytään tietoturvallisuuden kehittämistoimenpiteisiin, joita hallinnonalalla on toteutettu vv. 2021-2022.

Tilaratkaisujen turvallisuus

Ministeriön toimitilat sijoittuvat kokonaisuudessaan uudistetulle Merikasarmin kampukselle, jonne henkilöstö muutti väistötiloista asteittain vuodesta 2021 lähtien. Työtilat ovat valtionhallinnon nykykonseptin mukaisesti monitilakonseptin mukaisia monitiloja. Tilojen fyysinen turvallisuus on kulunvalvontoineen ja eriyttämisineen aivan eri turvallisuustasolla kuin aikaisemmat. Toisaalta monitilamalli soveltuu huonosti turvaluokitellun tietoaineiston käsittelyyn. Tässä suhteessa tiloihin onkin tehty ja tehdään vielä jonkin verran parannustoimenpiteitä. Ulkoministeriö on pyytänyt arviointia DSA-viranomaiselta (Designated Security Authority, osa NSA-verkostoa) ministeriön toiminnan ja toimitilojen soveltuvuudesta kansainvälisen korkeimmin turvaluokitellun tiedon käsittelemiseen. Toimintaprosessit ja fyysiset kontrollit ovat sinänsä läpäisseet asetetut vaatimukset.

Ulkomaanedustustojen osalta turvallisuustilanne on vaihteleva, sillä yhtenäistä turvaamiseen liittyvää kattavaa tilakonseptia ei ole aikaisemmin ollut kattavasti ja toisaalta se, millaiset tilat on kyetty ostamaan tai vuokraamaan vaikuttavat luonnollisesti turvaamismahdollisuuksiin. Rakenteelliset ja turvateknisten järjestelmien vaatimukset on kirjattu ulkomaanedustustojen rakenteellinen turvallisuusohjeeseen. Ohjeistuksessa on otettu huomioon tilan sijainti kansliassa ja sen mukaisesti riittävä sekä järkevä taso tarvittavalle suojaukselle. Peruskorjattavissa ja uusissa avattavissa edustustoissa turvalliset tilat saadaan järjestettyä hyvin, mutta olemassa olevien kanslioiden tilat joudutaan käymään läpi tapauskohtaisesti, jotta saadaan räätälöityä sopiva riittävän turvallinen tila. Toimintoja siirtämällä eri tiloihin ja tiivistämällä on löydetty pääosin tilat, jäännösriskit kohdekohtaisesti tarkastellen. Haastavinta on ääniseristyksen riittävä toteuttaminen ja tilan koko. Turvatekniikka tiloihin saadaan hoidettua kohtuullisesti.

Koettu hallinnonalan toimintaympäristön muutos ja uhkatekijöiden kasvu on aiheuttanut sen, että prioriteettijärjestystä edustustokohteiden osalta on tarkasteltu uudelleen. Tilanne aiheuttaa myös erityistä riskiperusteista tarkastelua muutamien edustustokohteiden järjestelyjen osalta. Hallinnollista turvallisuutta myös tarkasteltu ja parannettu sekä edustustojen tilaluokittelua viety eteenpäin tarkastelujakson aikana. Tarkastelujaksolla tiloihin on sovellettu vyöhykkeistämismallia sekä ministeriössä että edustustoissa, jota käytetään systemaattisesti myös uusien edustustotilojen suunnittelussa siten, että sisäkkäisten turvavyöhykkeiden totuttaminen mahdollistuu entistä paremmin.

Tietotekninen perusympäristö

Sekä perustietotekniikan kehittämiseen, että korkeamman turvatason toteutuksiin on vaikuttanut hidastavasti koettu pandemiajakso sekä osittain siitä johtuva globaali komponenttipula, joka on hidastanut sekä rajannut tarvittavan teknologian saatavuutta ja siten myös turvallisuuden parantamiseen liittyviä kehittämishankkeita.

Korkean turvaluokan tiedonhallinnan turvaaminen

[redacted]

Turvalliset videoneuvotteluratkaisut

[redacted]

Kiristynyt maailmanpoliittinen tilanne ja Suomen NATO-jäsenyys ovat nostaneet entisestään edustustojen tarvetta turvaluokiteltujen videoneuvottelupalvelujen ja muiden korkeamman turvaluokan järjestelmien käyttöön.

[redacted]

Turvallisen videoneuvotteluratkaisun levittämistä hidastaa joidenkin edustustojen tilojen pienuus sekä valittuihin neuvottelutiloihin tarvittavien TLIII-kriteereiden huomioiminen ja näihin liittyvien muutostöiden valmistuminen. Näiden rakenteellisen muutosten toteuttaminen tulee viemään aikaa ja niitä edistetään edustustojen muistakin syistä toteutettavien remontointien yhteydessä.

Mobiililaitteiden turvallisuus

[redacted]

Normaalien mobiililaitteiden (älypuhelimet, tablettilaitteet) osalta on tunnistettu tarve niihin asennettavaan turvallisen pikaviestintävälineeseen. Tarkastelujaksolla on testattu ratkaisua, mutta sen toimivuus ei ollut ulkomailla käytettävien liittymien osalta riittävä. Ratkaisua etsitään edelleen. Viestinnässä käytetään myös vapaasti ladattavaa Signal-sovellusta, mutta sen turvatasoa ei ole virallistettu.

NATO-liittymisprosessin tuomat kehittämistarpeet

NATO-liittymisprosessi on luonut uusia tarpeita turvalliseen tiedonhallintaan. Ministeriöllä on ollut tähänkin mennessä käytössään ratkaisuja, joiden välityksellä NATO:n turvaluokiteltua aineistoa on kyetty välittämään Suomeen. Jäsenyyden myötä tarpeet kuitenkin laajenevat sekä aineiston välitystarpeen, että NATO-yhteistoimintaan liittyvän kansallisen aineiston käsittelyn tarpeiden johdosta. Ulkoministeriö toimii jo nykyisellään eri kansainvälisten määräysten mukaisesti. Normaalissa ministeriön toiminnassa ei siis edellytetä suuria muutoksia, koska ministeriön toimintamallit ovat auditoidusti kansainvälisten tietoturvavelvoitteiden mukaisia.

[redacted]

[redacted]

[redacted]

[redacted]

Henkilöstön osaaminen

Ulkoasiainhallinnon henkilöstö on velvoitettu käymään säännöllisesti tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä verkkokoukutuksia. Niiden suorittaminen hyväksytysti on edellytyksenä käyttöoikeuksien säilymiselle hallinnonalan tietojärjestelmiin. Koulutukset ovat pääsääntöisesti verkkopohjaisia ja peruskoulutuksen lisäksi kokonaisuus sisältää erityiskursseja henkilöiden työtehtävistä riippuen.