Liikenne- ja viestintävaliokunta
00102 EDUSKUNTA
LiV@eduskunta.fi

8.2.2021

Asiantuntijalausunto

Asia: E 153/2020 vp Valtioneuvoston selvitys: EU-puheenjohtajamaan keskustelun avaus EU:n tasapainoisesta lähestymistavasta salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksien puitteissa

Kiitän mahdollisuudesta lausua asiantuntijana tästä asiasta. Annetussa muistiossa esitetty Suomen kanta on hyvä ja tasapuolinen, joskin melko ylimalkainen. On tärkeä huomioida seuraavat asiat lopullisen kannan muodostamisessa sekä jatkokeskusteluissa ja mahdollisessa tulevassa päätöksenteossa.

1) Salausmenetelmiin ei tule vaatia teoreettisella tasolla suunniteltuja “takaportti” -mekanismeja edes viranomaisten tarpeisiin
   a) Vaikka tällainen onnistuttaisiin suunnittelemaan, sen toteutuksen käyttäminen, käytön valvominen kansallisesti ja globaalisti sekä erityisesti tämän järjestelmän pääsyn valvonnan turvaaminen ovat äärimmäisen vaikeita ja ehkä jopa ratkaisemattomia ongelmia.
2) Salausta toteuttaviin ohjelmistoihin ja laitteisiin ei myöskään tule vaatia takaportteja samoin perustein. Tällainen vaatimus heikentää EU:n ja Suomen teknologista kilpailukykyä.
3) Käytännössä salattuihin tietoihin voidaan päästä yksittäistapauksissa kiinni muita reittejä, kuten pilvipalveluiden varmuuskopioiden, ohjelmistojen heikkouksien ja käyttäjien huolimattomuuden kautta.
4) Viranomaisten toimivaltuuksia tulee tarkastella niin, että ne ovat digitaalisessa maailmassa riittävät. Toimivaltuuksien tulee myös olla oikeasuhtaisia perusoikeuksien kanssa. Esimerkiksi Suomen tuoreissa tiedustelulaeissa on jo paljon menetelmiä, jotka saattavat vastata osaan tarpeista. Näiden menetelmien ja valtuuksien laajentamisessa tulee olla hyvin varovainen.
5) Viranomaisia tulee kouluttaa käyttämään työkaluja ja menetelmiä, jotka mahdollistavat todistusaineiston keräämisen yksittäistapauksissa. Työkaluja pitää myös olla saatavilla riittävästi, mikäli niiden käyttö katsotaan tarkoituksenmukaiseksi.

Alla on esitetty perusteluja näille näkökulmille sekä nostettu esiin muistiossa esiintyviä argumentteja ja niihin liittyviä huomioita.

Oulun yliopisto

PL 8000
90014 Oulun yliopisto

oulun.yliopisto @ oulu.fi
Puh 0294 480 000
Fax 08 344 064

www.oulu.fi

Salausmenetelmien kehitys ja toteuttaminen toimivat kahdella eri tasolla. ***Teoreettisella tasolla*** suunnitellaan menetelmiä (esim. Viestin salaus) ja esitetään matemaattiset perustelut (ns. turvallisuustodistus) niiden turvallisuudelle tiettyjen oletusten puitteissa. Oletukset koskevat esimerkiksi hyökkääjän laskentakykyä, eri osapuolten toimintaa ja muita käytettävissä olevia resursseja. Tällä tasolla järjestelmät pyritään aina osoittamaan täydellisen turvallisiksi eli että annettujen oletusten puitteissa hyökkääjä ei voi onnistua murtamaan salausta. Tämä tarkoittaa, että salauksen purkamiseen tarvitaan oikea salausavain ja ilman sitä purkaminen ei onnistu.

Toinen salausmenetelmien taso on ***käytännön järjestelmien ja laitteiden taso***. Tällä tasolla toteutetaan edellä mainittuja menetelmiä ohjelmoinnin ja elektroniikan keinoin. Nämä toteutukset ovat samanlaisia laitteita ja ohjelmistoja kuin mitkä tahansa muut digitaaliset laitteet ja ohjelmistot. Näin ollen niissä on myös samankaltaisia heikkouksia, kuten ohjelmointivirheitä, vääriä käyttötapoja, vanhentunutta teknologiaa jne. Mikä tahansa virhe tai heikkous tällä tasolla voi aiheuttaa salauksen tuoman hyödyn osittaiseen tai kokonaan menettämiseen. Näitä hyväksikäyttämällä myös viranomaiset voivat saada pääsyn yksittäistapauksissa (ja joskus laajemminkin) salattuun tietoon.

Usein käytetty esimerkki salatusta tiedosta on älypuhelimessa olevien tietojen salaaminen. Tällaiseen tietoon viranomaisilla saattaa olla tarve päästä käsiksi tutkinnan yhteydessä. Kuitenkin puhelimella oleviin salattuihin tietoihin ei nykyisin ole pääsyä muilla kuin puhelimen haltijalla (ei viranomaisilla eikä valmistajalla). Tämän tyyppinen salaus on usein toteutettu puhelimen lukituksen avulla. Nykyisin suosittu kasvojentunnistus puhelimen lukituksessa avautuu kuitenkin vain näyttämällä puhelinta henkilön kasvojen suuntaan. Tämän jälkeen puhelimen tiedot ovat saatavilla ja monet eri viestimien päästä päähän salatut viestit ja puhelimelle talletetut tiedot nähtävillä. Se, miten ja missä olosuhteissa tämän tyyppistä menetelmää voidaan hyödyntää viranomaisten toimesta, on poliittinen päätös, josta on hyvä käydä laajaa keskustelua. Vastaavan kaltaisia, yksittäistapauksissa toimivia menetelmiä, on varmasti tunnistettavissa muissakin tapauksissa, joissa salattu tieto on tutkinnallisesti tärkeää viranomaisille.

Muistiossa esitetään monia käsitteitä, joita ei ole määritelty riittävällä teknisellä tasolla, jotta niitä voitaisiin mielekkäästi analysoida ja kommentoida tekniseltä kannalta. Näitä käsitteitä ovat mm. *”tasapainoinen ja teknologianeutraali lähestymistapa”, ”tarkkarajaisesti määritelty mahdollisuus”, ”yksittäistapaus”* ja jopa *”vahva salaus”.*

Itse asiassa mikään tällä hetkellä käytössä oleva järjestelmä ei ole ristiriidassa muistiossa esitettyjen yleisluontoisten vaatimusten kanssa. Yksittäistapauksissa on usein mahdollista päästä käsiksi dataan ilman, että salausta on etukäteen heikennetty mahdollistamaan viranomaisten pääsy dataan. Tämä vaatii usein enemmän työtä, mutta on kuitenkin mahdollista esimerkiksi varmuuskopioiden kautta, käyttäjän laitteen salasanan tai muun kirjautumismenetelmän ohittamisella (kuten edellä mainittu kasvojentunnistus) tai ohjelmiston haavoittuvuutta hyödyntäen.

Viranomaisten toimivaltuuksien tarkastelu digitaalisessa maailmassa on varmasti tarpeen. On myös ensiarvoisen tärkeää, että viranomaisilla on käytössään työkaluja, joilla jo nyt voidaan saada todistusaineistoa

kerättyä myös salatuista laitteista ja viestinnästä. Koulutuksen tarve sekä työkalujen saatavuuden varmistaminen ovat tärkeitä kohtia huomioida tässä kehityksessä.

Kuitenkaan viranomaisille ei tule järjestää erillistä pääsyä salattuun tietoon itse salausmenetelmiin suunniteltujen mekanismien kautta. Tällaiset mekanismit luonnollisesti helpottaisivat viranomaisten työtä joissakin tapauksissa, mutta niiden aiheuttamat riskit, haitat ja vahingot laajemmin yhteiskunnassa ovat huomattavasti suuremmat kuin mahdolliset hyödyt.

Vaikka teoreettisesti ja teknisesti halutun kaltainen salausjärjestelmä voitaisiin toteuttaa, on erittäin epätodennäköistä, että sen käyttöä voitaisiin globaalisti vaatia ja valvoa. Lisäksi tämän järjestelmän avaimista ja niitä hallinnoivista henkilöistä ja organisaatioista ja niiden tietojärjestelmistä tulisi niin houkuttelevia kohteita tiedustelupalveluille, rikollisille ja muille tahoille, joilla on intressi päästä salattuihin tietoihin käsiksi, että näiden turvaaminen aukottomasti muodostuu liki mahdottomaksi ja äärimmäisen kalliiksi tehtäväksi.

Toinen kysymys on, voiko mikään taho vaatia poikkeuksia tähän salausjärjestelmään ja päästä käyttämään nyt jo tunnettuja menetelmiä, joihin ei ole tarkoituksellisesti rakennettu takaportteja. Mikäli ei, niin tällöin kaikkein salaisimpiinkin tietoihin ja viesteihin esim. Diplomaatti- ja sotilasviestintään pääsee käsiksi tuon järjestelmän kautta. Jos taas poikkeuksia sallitaan, niin mikä estää muitakin vaatimasta näitä poikkeuksia ja/tai käyttämästä vain noita aiemmin mainittuja menetelmiä. On mahdotonta valvoa ja selvittää esimerkiksi verkkoliikenteestä, mitkä viestit on salattu milläkin menetelmällä.

Näin siis päädytään hyvin vaikeisiin poliittisiin ja proseduraalisiin kysymyksiin. Tämä tarkoittaa, että halutun kaltaisen salausjärjestelmän avulla saatu ratkaisu tuskin olisi käyttökelpoinen reaalimaailman reunaehdot huomioon ottaen.

Edelleen tällainen mahdollinen vaatimus takaporteista on myös ristiriidassa vastikään voimaan tulleiden tiedustelulakien vaikuttavuusarvioinnissa esitettyjen argumenttien kanssa (ks. esim. HE 202/2017 vp) sekä myös Suomen kyberturvallisuusstrategian ja kyberturvallisuuden kehittämisohjelman tavoitteiden kanssa. Näin ollen on Suomen ja Euroopan etujen mukaista löytää muita menetelmiä ratkaista esitetyt ongelmat.

Lisäksi on hyvä huomata, että digitaalinen kommunikaatio jättää hyvin paljon tietoa viestinnästä, vaikka itse viestintä olisikin salattua. Tämä ns. ***metadata*** kertoo sen, kuka viestittää kenelle, kuinka usein, milloin, missä ja monia muita asioita. Näistä voidaan tehdä yleensä tarkkoja johtopäätöksiä ja päätelmiä, vaikka viestinnän sisältöön ei päästäkään käsiksi. Esimerkiksi henkilöllisyyden salaaminen verkossa on itse asiassa erittäin vaikeaa ja monesti hyvinkin anonyymejä menetelmiä käyttäneet tahot voidaan tunnistaa erilaisen metadatan perusteella.

Riippumatta siitä, minkälaisia teknisiä ja muita ratkaisuja päädytään toteuttamaan, pääsy salattuun tietoon tulee rajata ja siksi seuraava lainaus muistiosta on erinomaisen tärkeä ja sen toteutumista tulee seurata keskustelun edetessä.

“Toimivaltaisten viranomaisten pääsy salattuun tietoon on rajattava esimerkiksi rikollisuuden vakavuuden perusteella. Lisäksi EU-tason ratkaisussa on varmistuttava kansallisten laillisuusvalvontaviranomaisten edellytyksistä valvoa viranomaisten toiminnan lainmukaisuutta.“

Kun keskustelua tästä aiheesta jatketaan eri toimijoiden kesken ja erilaisilla forumeilla, edellä mainituista argumenteista voi olla hyötyä. Olen myös henkilökohtaisesti mielelläni mukana keskustelussa ja autan asiantuntemuksellani päätöksenteossa.

Oulussa 8.2.2021

Kunnioittavasti,

Kimmo Eerik Halunen

Digitally signed by Kimmo Eerik Halunen
DN: cn=Kimmo Eerik Halunen, ou=TSTK, email=Kimmo.Halunen@oulu.fi
Date: 2021.02.09 12:23:44 +02'00'

Kimmo Halunen
Professori
Kyberturvallisuus
Oulun yliopisto ja Maanpuolustuskorkeakoulu