Eduskunta

Liikenne- ja viestintävaliokunta

F- Securen lausunto: 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

F-Secure kiittää mahdollisuudesta lausua ja tuoda asiantuntijanäkemystään EU-puheenjohtajamaan keskustelun avaukseen EU:n tasapainoisesta lähestymistavasta salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksien puitteissa.

Luotettava salausteknologia on yhteiskunnan turvallisuuden, yksityisyydensuojan ja ihmisoikeuksien toteutumisen ja digitaalisten palveluiden luottamuksen kulmakivi. Viimeaikaisten tapausten (Vastaamo, eduskunnan tietovuoto, SolarWinds) valossa käymme parhaillaan kansallisesti keskustelua kyberturvallisuuden vahvistamisesta ja kriittisten tietovarantojen ja infrastruktuurin suojaamisesta.

Ymmärrämme edessämme olevan haasteen ja huolen lainvalvonnan mahdollisuuksista tutkia ja selvittää vakavia rikoksia, kuten terrorismi, järjestäytynyt rikollisuus ja lasten seksuaalinen hyväksikäyttö, myös digitaalisessa ympäristössä.

Niin kansallisesti kuin EU:ssa on käsittelyssä useita kyberturvallisuuteen liittyviä aloitteita ja näistä tulisi keskustella ja eri vaihtoehtoja punnita kokonaisuutena. Nyt keskustelua käydään eri foorumeilla ja näiden eri toimijoiden näkökulmasta ja tarpeesta käsin. Haasteena on myös teknisen ratkaisun kehittäminen monitoimijaympäristössä, jossa on toimijoita avoimen lähdekoodin kehittäjistä monikansallisiin yhtiöihin ja valtiollisiin toimijoihin.

Salausteknologioiden kehittämisessä ja käytössä on muutamia teknisiä ja teknologiaan liittyviä perusperiaatteita, jotka on tärkeää huomioida, kun mietitään ratkaisuja ja punnitaan poliittisia ja arvovalintoja.

1. Salaus pyrkii aina olemaan murtamatonta (informaatioteoreettisesti salatusta viestinnästä ei saisi paljastua sen enempää tietoa kuin kohinasta). Kaikki tavat, joilla salatusta tiedosta kyetään saamaan informaatiota muille kuin niille, joille se on tarkoitettu, ovat salauksen heikkoutta, joka pyritään poistamaan.

2. Edellä olevaa perusperiaatetta eivät määritä ideologiset tarkoitusperät vaan se, että vahvan salauksen luominen on jo itsessään erittäin vaikeaa. Valikoivasti tietoa ulos antavan salausmenetelmän tekeminen on vielä vaikeampaa, koska siinä pitää huolehtia salauksen lisäksi myös pääsynhallinnasta, esimerkiksi viranomaisavainten jakamisesta. Tämä on salauksen normaalin tavoitteen näkökulmasta poikkeama. Järjestelmäsuunnittelu pyrkii eliminoimaan poikkeamat myös siksi, että monimutkaisuus kasvattaa järjestelmän hyökkäyspinta-alaa ja kyberuhkien riskiä.

3. Käytetyt salaustekniikat (algoritmit) ja yhteyskäytännöt (protokollat) ovat usein maailmanlaajuisia standardeja ja niillä on tarkkoja yhteensopivuusvaatimuksia. Nykyaikaiset algoritmit ja protokollat on myös enenevässä määrin suunniteltu niin, että jälkikäteinen salatun viestin avaaminen olisi myös mahdotonta, elleivät viestinnän osapuolet ole aktiivisesti olleet

mukana koko viestinnän ajan. Tällä pyritään estämään järjestelmistä varastettujen salausavainten käyttöä aiemman viestinnän avaamiseen. Näistä syistä itse salaukseen puuttuminen vaatisi laajoja teknisiä muutoksia ja maailmanlaajuista harmonisointia.

4. Vaikka pääsy salattuun tietoon saataisiinkin teknisesti toteutettua, seuraava kysymys olisi poliittinen eli kenelle ja missä tapauksissa tietoa salatusta tiedosta voidaan antaa. Tämän vastauksen pitäisi olla sovellettavissa maailmassa, jossa järjestelmiä kehitetään, jaellaan ja käytetään kaikkialla maailmassa sekä kaupallisesti että ei-kaupallisesti. Esimerkiksi älypuhelimen hypoteettisen pikaviestisovelluksen viestinnän osalta yhtälössä mukana saattaisivat olla Yhdysvalloissa ja Kiinassa sijaitsevat sovelluskaupat ja matkapuhelinvalmistajat, ryhmä yksityishenkilöitä avoimen lähdekoodin sovelluskehittäjänä ja keskenään erilaisissa maissa toimivat viestinnän osapuolet.

Kuten yllä on kuvattu, tekniset, kaupalliset ja poliittiset intressit eivät nykytilanteessa mahdollista salauskäytäntöjen tavoitteiden muuttamista. Muistiossa mainittu turvallisuus "salauksen avulla ja salauksesta huolimatta" tarkoittaa, että mikäli muulle kuin viestinnän osapuolelle pitäisi antaa pääsy tietoon, sen olisi teknisesti tapahduttava salatun tiedonsiirron tai tallennuksen ulkopuolella (eli ennen salausta tai salauksen purun jälkeen).

Muistiossa käsiteltävän salattuun tietoon pääsyn rinnalla olisi tärkeää pohtia ja valmistella myös ennaltaehkäiseviä toimia, jotka saattaisivat osaltaan auttaa. Nämä voivat olla ei-teknisiä, esimerkiksi yhteiskunnallisia, keinoja tai teknisesti esimerkiksi koneoppimiseen pohjautuvia ratkaisuja, jotka voisivat prosessoida tietoa silloin, kun sitä ei ole salattu.

Muistiossa todetaan, että EU pyrkii luomaan aktiivisen keskustelun teknologiateollisuuden sekä tutkimuslaitosten ja korkeakoulujen kanssa varmistaakseen vahvan salausteknologian jatkuvan kehityksen ja käytön. On tärkeää, että myös suomalaisia asiantuntijoita saadaan näihin pöytiin. Meillä on useita asiantuntijoita niin elinkeinoelämän kuin korkeakoulujen ja tutkimuslaitosten piirissä.

F-Secure tarjoaa salattuja yhteyksiä tuottavia tuotteita (esim. Freedome VPN kuluttajille) sekä konsultoi julkisen ja yksityisen sektorin toimijoita tietoturvassa Suomessa, Euroopassa ja kansainvälisesti useissa eri maissa. Tietoturva-alan yrityksen näkökulmasta asiakastarve on selkeä: riskinhallinta ja kriittisen tiedon ja tietojärjestelmien suojaaminen. Tähän vaaditaan ratkaisuja, joista voidaan mahdollisimman yksiselitteisesti todeta ratkaisun tarjoaman tietoturvan taso ja vaikutus riskiin. Asiakkaan tietoturvariskiarvio on hankala yhtälö jo nykyisellään. Valikoitu ylimääräinen pääsy salattuun tietoon tai muu informaation hallittu jakaminen lisää monimutkaisuutta entisestään. Ulkopuolelta tuleva poliittinen muuttuja, joka vielä vaihtelisi maittain, tekisi jäännösriskin arvioinnista erittäin vaikeaa. F-Secure haluaa jatkossakin kehittää ja tarjota kansallisesti ja globaalisti sellaisia tuotteita ja ratkaisuja, jotka ovat teknisesti mahdollisimman selkeitä ja luotettavia ja jotka ennustettavasti eliminoivat riskitekijöitä.

F-Secure osallistuu mielellään asian jatkovalmisteluun ja teknisiin keskusteluihin niin kansallisesti kuin EU:n asiantuntijaryhmissä.

Kunnioittavasti,

Nina Hyvärinen

Yhteiskuntasuhdejohtaja

F-Secure Corporation