Effin lausunto: Vahva salaus paras turva kansalaisille

LAUSUNTO
15.2.2021
Asia: E 153/2020 vp

Asiantuntijalausunto: “Keskustelun avaus EU:n tasapainoisesta lähestymistavasta salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksien puitteissa”

Electronic Frontier Finland – Effi ry kiittää mahdollisuudesta tulla kuulluksi asiassa.

Effi on vuonna 2001 perustettu kansalais- ja asiantuntijajärjestö, joka puolustaa perus- ja ihmisoikeuksia digitaalisessa toimintaympäristössä. Näkökulmamme on erityisesti sähköisiä palveluja käyttävän kansalaisen tietosuojaa ja perusoikeuksia painottava.

Effin kanta

Toimiva salaus takaa sen, että ulkopuolisilla ei ole pääsyä viestien sisältöön. Keskustelun avauksessa tosiasiallisesti vaaditaan takaovea salaukseen. Käsiteltävä asia on esitelty huolellisesti sanomatta tätä suoraan. *“EU:n tasapainoisesta lähestymistavasta salaukseen”* hakee lähtökohtaisesti toimenpiteitä vastustaa toimivaa turvallista salausta.

Tässä lausunnossa keskitymme päästä päähän salauksen käsittelyyn, koska se on ollut EU:ssa keskustelussa. Toki salausta on monenlaista ja esimerkiksi toimiva tiedostojen salaaminen tallennuslaitteille on toinen tärkeä tapa turvata kansalaisten turvallisuutta.

Salaus on moderni tapa varmistaa yksityisyys verkossa ja edistää kansalaisten oikeuksia. Effin ja muiden järjestöjen huoli on, että päästä päähän salaavien turvallisten pikaviestinten käytön rajoittaminen, kieltäminen tai pääsy viestintään vain heikentää entisestään kansalaisten hyvinvointia ja turvallisuutta.

Ehdotetut takaportit viestimiin [1] johtavat laaja-alaisesti turvallisuuden heikkenemiseen koko maailmassa. Pikaviestimien turvallisuuden heikentämisestä on keskustelu myös EU:ssa [2].

EU:n ja sen jäsenvaltioiden on edistettävä päästä päähän -salauksen käyttöönottoa viestimissä ja viestinnän yksityisyyttä. Pikaviestimiä kehittäviä organisaatioita tulee kannustaa päästä päähän -salauksen lisäämiseen viestimiin ja tarjota läpinäkyvyyttä varmentaa, että salaus suojaa viestit vain vastaanottajan ja lähettäjän väliseksi. Tämä suojaa ihmisiä parhaiten viestinnän vakoilulta ja vaalii kirjesalaisuutta.

Miksi Effin kanta asiaan saattaa kuulostaa mustavalkoiselta?

Keskustelun pohjana on “EU:n tasapainoisesta lähestymistavasta liittyen salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon toimivaltuuksien puitteissa.”

Ikävä kyllä teknisesti salaus joko toimii tai siihen on pääsy. Mikäli esimerkiksi WhatsApp loisi takaportin viestinnän lukemiseen EU:n viranomaista varten vain vakavien rikosten selvittämiseksi, tätä samaa takaporttia tulisivat käyttämään myös EU:n ulkopuoliset maat. Lisäksi mikään tekninen rajoite ei estä käyttämästä tätä takaporttia massavalvontaan.

Vahva salaus nykymaailmassa

Pikaviestimien turvallisuuden heikentämisestä on keskustelu myös EU:ssa. Effi haluaa muistuttaa päästä päähän -salauksen yhteiskuntaa parempaan suuntaan vievästä voimasta. Effi muistuttaa myös takaporttien ja heikennysten tuomista mittavista ratkaisemattomista ongelmista.

Päästä päähän -salauksella viestintä salataan lähettäjän päätelaitteella ja avataan vasta vastaanottajan laitteella siten, ettei kukaan muu kuin vastaanottaja ja viestin lähettäjä pääse lukemaan viestejä. Edes palveluntarjoaja ei pääse viestejä lukemaan. Näin toimii esimerkiksi WhatsApp-pikaviestin, jossa liikkuvia viestejä WhatsApp-pikaviestintä tarjoava yhtiö ei pääse itse lukemaan.

YK:n ihmisoikeuksien yleismaailmallinen julistus takaa sananvapauden ja yksityisyyden. Kirjesalaisuus on useiden maiden, kuten Suomen, perustuslaissa. Päästä päähän -salaus on konkreettisin tapa turvata kirjesalaisuus nykyaikaisessa sähköisessä viestinnässä. Päästä päähän -salaus suojelee kirjesalaisuutta myös viestiä välittävän palvelun urkinnalta. Tällöin viestejä eivät pääse myöskään lukemaan eri maiden viranomaiset tai järjestelmiin tietomurron kautta tunkeutuneet vakoojat.

Pelkästään WhatsAppin päästä päähän -salauksen avulla yli miljardi viestimen käyttäjää luottaa päivittäisen arkaluontoisenkin viestintänsä kulkemaan teknologiayhtiön kautta. Koska WhatsApp ja monet muut pikaviestimet suojaavat käyttäjiä urkinnalta, niin 7 maata maailmassa on kieltänyt tai rajoittanut näiden pikaviestinten käyttöä:

- Pohjois-Korea
- Kiina
- Syyria
- Yhdistyneet arabiemiirikunnat
- Iran
- Qatar
- Kuuba

Näissä maissa turvallisen ja yksityisen viestinnän käytön rajoittamista on perusteltu kansallisella turvallisuudella, terrorismin torjunnalla ja lasten suojelulla.

1. Päästä päähän -salaus takaa nykypäivän kirjesalaisuuden

Teknologiayhtiöille ei ole haluttu antaa portinvartijan roolia miljoonien ihmisten yksityiseen viestintään. Tähän on ratkaisuna päästä päähän viestinnän salaavat pikaviestimet. Tällöin vain viestin lähettäjä ja vastaanottaja voivat lukea viestejä. Viestejä välittävä yritys tai verkkoa vakoilevat rikolliset eivät pääse lukemaan viestejä matkalla. Näin poistetaan välistä mahdollisuus vakoiluun. Viestimen turvallisuus ja yksityisyys on luotettavampi.

2. Viestimien turvallisuuden alentaminen takaportilla vaarantaa demokratiaa ja vapautta

Oikeus yksityiseen keskusteluun on perusoikeus kansainvälisissä sopimuksissa ja länsimaisessa perinteessä. YK:n ihmisoikeuksien yleismaailmallinen julistus takaa sananvapauden ja yksityisyyden. Kirjesalaisuus on myös useiden maiden, kuten Suomen, perustuslaissa.

3. Pääsyä viestintään takaportin kautta vaativat myös totalitaristiset hallinnot

Mikäli pikaviestintä hallinnoiva yhtiö, kuten Facebook, luo takaportin viestien lukemiseen Yhdysvaltojen hallintoa varten, myös Kiina ja Valko-Venäjä vaativat samaa pääsyä viesteihin. Käytännössä pääsyä ei voida rajata vain yhden maan tai valittujen maiden viranomaisille, koska yritykset joutuvat noudattamaan myös muiden maiden lainsäädäntöä toimiessaan niiden alueella.

4. Takaportti helpottaa myös rikollisten pääsyä viestintään ja sen laitonta hyödyntämistä

Kun pääsyä jaetaan monelle viranomaiselle useassa maassa, niin pääsy takaportin kautta viestintään voi vuotaa ulkopuolisille. Takaportti viestintään myös heikentää teknisesti järjestelmän luotettavuutta ja sen kautta on teknisesti mahdollista laittomasti murtautua vakoilemaan viestintää.

5. Yritykset huonoja portinvartijoita kansalaisten viestinnälle

On haitallista tehdä yrityksistä, kuten Facebookista, pääsynhaltija yli miljardin ihmisen yksityiseen viestintään. Yli miljardin ihmisen viestintään olisi takaportin kautta pääsy yksityisen yrityksellä. Facebookilla on omat taloudellliset kannusteensa hyödyntää yksityisten viestien tietoja.

6. Rikolliset voivat aina valita viestimiä, joissa ei ole takaportteja

Vahvoja salausmenetelmiä käyttäviä viestimiä on ollut tarjolla jo vuosikymmeniä ja ne ovat jatkossakin saatavilla. Rikolliset tulisivat valitsemaan sellaisia tunnettuja viestintätapoja, joihin takaportteja ei olisi asennettu. Näin heikennykset kohdistuisivat tavallisten kansalaisten viestintään.

7. Tunnetut salausmenetelmät pysyvät edelleen käytössä jatkossakin

Yksinkertaisen viestien salausjärjestelmän valmistaminen on mahdollista käyttäen tunnettua oppikirjamateriaalia salauksesta. Näin ollen uusia salausjärjestelmiä on tarjolla jatkossakin. Tämä johtaisi kahtiajakoon, jossa teknisesti valveutuneet ihmiset suojaisivat edelleen viestintänsä tehokkaasti, mutta suuri osa aivan tavallisista ihmisistä päätyisi käyttämään suosituimpia turvattomampia viestimiä.

Yksityiskohtaiset perustelut: miksi kyseessä on aina takaportti

Teknisesti pääsyä salattuun viestintään ei voida rajata vain tiettyyn käyttötarkoitukseen. Viestintä tapahtuu maailmanlaajuisesti ja EU ei voi päättää, miten muut maat päättävät hyödyntää pääsyä viestintään. Tämä ongelma on riippumaton toteutusteknologiasta.

EU:n pöydällä ollut tekninen suunnitteluluonnos [3] ei sisällä yhtään merkittävää parannusta tilanteeseen, että salaus joko toimii tai sitten viestintään annetaan pääsy ulkopuolisille.

Pääsymekanismi	**Analoginen selitys**	**Pääsyn laajuus**	**Väärinkäyttö**
Palveluntarjoaja pääsee viestintään ja voi jakaa pääsyn ulkopuolisille. Oikeuden päätöksellä määrätään pääsy viestintään.	Tuomari määrää pääsyn tiettyjen henkilöiden viestintään. Palveluntarjoaja lukee viestit.	Maassa maan tavalla. Viranomaisilla laaja pääsy viestintään. Palveluntarjoaja voi lukea ja hyödyntää viestejä.	Ihmisoikeustilanteen mukaan hyvin laaja monissa maissa. Ei teknisiä rajoitteita väärinkäyttöön. Rikollisten tietomurto järjestelmiin.
Homomorfinen salaus. [Huom. teknologia vasta kehitteillä.]	Salausta purkamatta mahdollista lukea tiettyjä	Jokainen maa voi tietysti vaatia seulontaan sellaista sisältöä	Ihmisoikeustilanteen mukaan hyvin laaja monissa maissa.

	tunnusmerkkejä viestinnän sisällöstä. Ikään kuin vesileima viestinnän päällä luettavissa.	kuin haluaa. Teknologia rajoittaa seulonnan tehokkuutta, mutta ei rajaa sen kohdistamista vain vakaviin rikoksiin.	Teknologia ei rajaa käyttöä vain vakavien rikosten seulontaan. Palveluntarjoaja voi hyödyntää viestien sisällön tunnusmerkkien lukemista.
Seulonta päätelaitteella. Seulontaperiaatteet valitsee viranomainen. Seulontaa voi tehdä myös palveluntarjoja.	Päätelaite, esimerkiksi älypuhelin, lukee viestit ennen kuin ne lähetetään eteenpäin salattuna.	Kaikki viestit luettavissa kohteina olevilta henkilöiltä tai kaikilta.	Ihmisoikeustilanteen mukaan hyvin laaja monissa maissa. Palveluntarjoja voi hyödyntää omiin tarkoituksiinsa.
Tarkastussummiin (hash) perustuva tiedon seulominen.	Lasketaan esimerkiksi kuvaa tai sanaa vastaava lyhyt tarkastussumma ja seulotaan viestinnästä osumat.	Tarkastussummia voidaan lisätä mille tahansa sisällölle. Teknologia ei rajoita seurannan laajuutta.	Ihmisoikeustilanteen mukaan hyvin laaja monissa maissa. Palveluntarjoja voi hyödyntää omiin tarkoituksiinsa.
Seulonta kolmannen osapuolen *luotetussa* ympäristössä. [Huom. vaikka teknisesti on rakennettavissa suljettuja laskentajärjestelmiä, niin järjestelmän ylläpitäjä määrää pelisäännöt.]	*Luotettu* kolmas osapuoli seuloo viestintää. Ikään kuin kirje lähetetään hyvin luotettuun paikkaan ja tarkistetaan sisältö siellä.	Kolmas osapuoli voi seuloa mitä vain ja se voidaan etenkin velvoittaa seulomaan millä vain laajuudella viestintää.	Meillä ei ole maailmanlaajuista luotettua kolmatta osapuolta. Ihmisoikeustilanteen mukaan hyvin laaja monissa maissa.

Edellä esitellyt ratkaisut ovat olleet esillä EU:n suunnitteluluonnoksessa "Technical solutions to detect child sexual abuse in the end-to-end encrypted communications" [3]. Myös tekniikoiden yhdistelmiä on läpikäyty, mutta lopputulos tarkoittaa aina kolmannen osapuolen laajaa pääsyä viestintään.

Esitetyt tekniset tavat johtavat aina laajaan pääsyyn kaikkien viestintään ympäri maailmaa. Käytännössä ei voida puhua vahvasta toimivasta turvallisesta salauksesta. Lisäksi on mahdollista, että palveluntarjojaan kohdistuu tietomurto, joka mahdollistaa laajan pääsyn koko palvelun käyttäjien viestintään.

Ratkaisuehdotus

Ongelmien ratkomiseen on aina muita, parempia keinoja kuin viestinnän vakoilu. Lastensuojelua, terrorismia tai järjestäytynyttä rikollisuutta ei saa käyttää verukkeena heikentää viestinnän yksityisyyttä ja viestimien turvallisuutta.

Yksityinen turvallinen viestintä edistää yhteiskuntaa paremmin kuin heikennykset salaukseen ja takaporttien pääsy viestisisältöihin.

Päästä päähän -salaus itse asiassa edistää sellaista yhteiskuntaa, joka takaa turvallisuuden kaikille.

Kansalaisia turvaa ja rikollisuutta vähentää parhaiten yhteiskunnan kehittäminen vakaammaksi:

- Rauha yhteiskunnassa ja konfliktien välttäminen.
- Oikeusvaltiokehitys, hyvinvoinnin kasvu ja kansalaisten mahdollisuudet edistää hyvinvointiaan.
- Erityisesti lapsia suojeleva lainsäädäntö ja väkivallan kriminalisointi sekä lapsia suojelevat kansainväliset sopimukset.
- Oikeusvaltion, demokratian ja tietoturvan edistäminen suojelee kaikkia kansalaisia paremmin kuin yritysten, rikollisten ja valtioiden pääsy yksityisiin viesteihin.
- Salauksen turvaama yksityinen viestintä edistää lopulta maailman valtioita kehittymään sellaisiksi, että ongelmia ei ratkota valvomalla ihmisten viestintää.

Näitä päämääriä Effi ja muut kansalaisjärjestöt haluavat edistää.

Electronic Frontier Finland – Effi ry
Juha Nurmi ja Mikko Kenttälä, Effin tietoturvatyöryhmä

[1] https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety

[2] https://www.eff.org/deeplinks/2020/10/orders-top-eus-timetable-dismantling-end-end-encryption

[3] https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

Lisätietoja:
Juha Nurmi
Electronic Frontier Finland – Effi ry
040 506 8305
juha.nurmi@effi.org

Mikko Kenttälä
Electronic Frontier Finland – Effi ry
040 746 5501
mikko.kenttala@effi.org

Electronic Frontier Finland – Effi ry on perustettu puolustamaan kansalaisten sähköisiä oikeuksia. Tällaisia ovat esimerkiksi oikeus sensuroimattomaan viestintään, kohtuullisiin käyttöehtoihin digitaalista sisältöä ostettaessa sekä vapaus kehittää ja julkaista avoimia tietokoneohjelmia. Yhdistys herättää keskustelua ja pyrkii vaikuttamaan muun muassa lainsäädäntöhankkeisiin sananvapaudesta ja tekijänoikeudesta Suomessa ja Euroopassa. Mielestämme yksityisyyttä ei saa rikkoa, spämmäys tulee kieltää ja ohjelmistoideapatenteista on enemmän haittaa kuin hyötyä. Yhdistyksellä on noin 1600 jäsentä. Lisätietoja Effin kotisivulta www.effi.org.