Electronic Frontier Finland – Effi ry

Lausunto 16.10.2024

Asia: U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final).

Electronic Frontier Finland – Effi ry kiittää Liikenne- ja viestintävaliokuntaa mahdollisuudesta tulla kuulluksi otsikon asiassa.

Yhteenveto:

- Järjestelmä muodostaisi massiivisen tietoturvariskin. Niin rikolliset kuin valtiollisetkin toimijat, erityisesti erilaiset tiedustelupalvelut, pyrkisivät varmasti käyttämään sitä väärin, ja kyllin suurilla resursseilla se varmasti myös onnistuisi.
- Esitys tosiasiallisesti rikkoisi päästä-päähän salauksen: vaikka salausta ei murrettaisi vaan se kierrettäisiin tai sen käyttö estettäisiin, vaikutus olisi sama.
- Kyseessä olisi Euroopan tuomioistuimen kieltämä massavalvonta: määräyksen kohteeksi joutuneessa palvelussa kaikkien käyttäjien viestit pitäisi analysoida ilman kohdennettua epäilyä.
- Rikolliset pääsisivät käsiksi materiaalin tunnistukseen käytettävään tunnistetietokantaan ja pystyisivät kiertämään sen - myös alustoilla joilla tunnistus nyt toimii.
- Esitys ei puutu varsinaiseen ongelmaan CSA -materiaalin levittämisessä, se vain ajaa materiaalin levittäjät hajautettuihin palveluihin.

Esityksen tietoturvaongelmat

Takaovi

Puheenjohtajanvaltion ehdotuksessa ehdotetaan, että mikäli päästä-päähän salauksen toteuttavalle viestintäsovellukselle annettaisiin määräys automaattisen tunnistamisen käyttöönotosta, tulisi tämä tunnistaminen suorittaa itse sovelluksessa, ennen kuin sen kohteena oleva kuvamateriaali salataan tiedonsiirtoa varten.

Tämä on merkittävä tietoturvariski.

Ehdotuksen mukaan tunnistaminen tehtäisiin käyttäen komission määrittelemiä tekniikoita - oleellisesti tämä tarkoittaisi komission toimittamaa sovelluskirjastoa, joka liitettäisiin osaksi kohdesovellusta. Tämä sovelluskirjasto käyttäisi EU-keskuksen tuottamia ja ajan tasalla pitämiä tunnisteita tunnistamaan salaista materiaalia.

Tarkemmin sanoen tunnisteilla tarkoitettaneen yksisuuntaisia visuaalisia tiivistefunktioita hyödyntäviä tekniikoita. Esimerkkeinä Microsoftin PhotoDNA, Googlen CSAI ja Facebookin TMK.

Tällainen sovelluskirjasto, jonka toimintaperiaate on salainen, on loppukäyttäjän tai sovelluksen turvallisuutta arvioivan asiantuntijan näkökulmasta läpinäkymätön laatikko, jonka turvallisuudesta ei voida varmistua. Olennaisesti sovellukseen upotettava vakoiluohjelma.

Vaikutus on suurin kaikkein turvallisimmille päästä-päähän salatuille sovelluksille, joissa sovelluksen koko toiminta on varmennettu julkaisemalla lähdekoodi ja binäärikoodin tuottamismentelmä niin, että ne ovat

läpinäkyvästi kaikkien varmennettavissa. Tällainen ylimääräinen lisäkomponentti romuttaisi oleellisesti tämän viestivälineen kaikkein tärkeimmän turvallisuustakeen.

Kolmannen osapuolen ei tarvitse olla pahantahtoinen, että tällainen ylimääräinen kirjasto muodostaisi tietoturvariskin. Nykyaikana yksinkertainenkin sovelluskomponentti koostuu niin monesta eri lähteestä tulevasta palasesta ja niiden kokoaminen toimivaksi sovellukseksi koostuu niin monesta eri vaiheesta, että koko prosessin varmistaminen turvalliseksi on merkittävä haaste. Tällaisista toimitusketjuhyökkäyksistä on lukemattomia esimerkkejä viime vuosilta.

Esimerkiksi Hollannin tiedustelu- ja turvallisuuspalvelu AIVD on ilmaissut pitävänsä tällaisen ylimääräisen ei-julkisen sovelluskomponentin aiheuttamaa hyökkäyspinta-alaa liian vaikeana turvattavaksi luotettavasti.

"Skannaussovelluksen asentaminen kaikkiin matkapuhelimiin ja siihen liittyvine infrastruktuuri- ja hallintaratkaisuuineen johtaa laajaan ja hyvin monimutkaiseen järjestelmään. Tällainen monimutkainen järjestelmä antaa pääsyn suureen määrään mobiililaitteita ja niissä olevia henkilötietoja. Syntyvä tilanne on AIVD:n mielestä liian suuri riski digitaaliselle resilienssillemme. [...] Tunnistamismääräysten soveltaminen päästä päähän -salatun viestinnän tarjoajiin sisältää liian suuren tietoturvariskin digitaaliselle kestävyydellemme."

https://berthub.eu/articles/posts/dutch-intel-service-csam-update/

Sisäministeriön lausunnossa tällaista ylimääräistä sovelluskirjastoa on verrattu virustorjuntaohjelmaan. Vertaus on osuva. Pitkiin aikoihin vakavastiotettavat turvallisuusohjeistukset eivät ole sallineet virustorjuntaohjelmia sisällytettäviksi korkean turvallisuuden järjestelmiin. Niiden avaama hyökkäyspinta-ala on yksinkertaisesti liian suuri.

Mainittakoon vielä, että Apple hylkäsi oman suunnitelmansa vastaavanlaisesta suodatuksesta jo aikaisemmin todeten, ettei pysty toteuttamaan sitä turvallisesti.

Tunnistetietojon vuoto

Toinen tietoturvariski muodostuu siitä, että etenkin sijoitettuna avoimen lähdekoodin viestintäsovellukseen, voi tällainen sovelluskirjasto auttaa rikollisia kiertämään koko suodatusmekanismin.

Ongelman ydin on, että kun tunnistamismääräys annettaisiin, on olemassa riski, että rikolliset voivat kopioida tunnistuksen tekevän sovelluskirjaston ja tunnisteet sovelluksesta ja käyttää niitä tarkistaakseen etukäteen, mikä materiaali jää tunnistimeen ja muuttaa kyseistä materiaalia niin, ettei se enää jää kiinni mihinkään tunnistimeen, joka käyttää näitä samoja tunnisteita.

Tämä vaarantaisi nyt käytössä olevan - verkkoalustojen vapaaehtoisuuteen perustuvan - suodatuksen toimivuuden.

Kun sovellus on avointa lähdekoodia, voi sen toimintaa muokata helposti. Esimerkiksi sillä tavoin, että se ei enää ilmoitakaan positiivista tunnistuksista viranomaiselle vaan sen sijaan sovelluksen paikalliselle käyttäjälle. Samoin se voidaan muokata skannaamaan kaikki käyttäjän haluamat tiedostot.

Esimerkiksi PhotoDNA tunnistimen tunnistusmekanismi voidaan kiertää tehokkaasti muuttamalla vain pieni osa kuva-alasta - jos tämä osa onnistutaan valitsemaan oikein. Tämä ei ole merkittävä ongelma, jos käyttäjä ei tiedä varmasti mitä osaa kuvasta on tarpeen muokata. Sen sijaan ongelmasta tulee merkittävä, jos käyttäjä voi jokaisen muokkauksen jälkeen testata toimiko se vai ei.

PhotoDNA:n toimintaa on avattu tarkemmin oheisella sivulla:

https://hackerfactor.com/blog/index.php?/archives/931-PhotoDNA-and-Limitations.html

Uhka ei poistu sillä, että tunnisteita päivitetään jatkuvasti, eivätkä vanhat tunnisteet välttämättä ole hyödyllisiä pitkän aikaa. Rikollinen saa uudet päivitetyt tunnisteet omaan sovellukseensa samaan aikaan kuin ne tulevat käyttöön muidenkin käyttäjien sovelluksissa.

Tätä riskiä ei ole mahdollista kiertää muuten, kuin tekemällä sovelluskirjastosta itsenäinen komponentti, joka kommunikoi suoraan taustajärjestelmän kanssa, eikä sen viestintäsovelluksen kanssa johon se on sijoitettu. Tällöin olisi kyseessä oleellisesti erilainen ratkaisu kuin nyt ehdotettu. Sillä olisi suuremmat perusoikeusvaikutukset, eikä näitä oikeusvaikutuksia ole käsitelty puheenjohtajavaltion ehdotuksessa.

Huono valmistelu

Tähän liittyen paljastuukin ehdotuksesta vielä perustavanlaatuisempi tietoturvaan liittyvän ongelma. Edellä mainittu tietoturvariski on kenen tahansa tietoturvaa ymmärtävän triviaalisti havaittavissa, mikäli tämä perehtyy esityksen sisältöön kunnolla. Kuitenkaan kyseistä riskiä tai sen torjuntakeinoja ei ollenkaan mainita puheenjohtavavaltion ehdotusversion resitaaleissa. Tästä voidaan päätellä, että ehdotuksen tietoturva-analyysi on kiireen takia tai muista syistä jäänyt pahasti puutteelliseksi.

Tämä asettaa kaikki ehdotuksessa esitetyt tietoturvaväitteet varsin kyseenalaiseen valoon.

Perusoikeusvaikutukset

Massavalvonta

Puheenjohtajavaltion ehdotukseen sisältyvä mahdollisuus määrätä viestintäsovellukset suorittamaan automaattista tunnistamista käyttäjien välittämään kuvamateriaaliin on edelleen kiellettyä massavalvontaa. Määräys koskee kaikkia palvelun käyttäjiä - ei pelkästään niitä, joita epäillään rikoksesta. Skannauksen kohteena on kaikki käyttäjän välittämä kuvamateriaali. Massavalvonnan laillisuuden kannalta ei ole eroa sillä tekeekö valvontaa viranomainen itse vai palveluntarjoaja viranomaisen velvoittamana.

Nämä perusoikeuksien rajoitukset eivät ole tehokkaita, välttämättömiä tai oikeansuhtaisia.

Ehdotuksessa ja siitä annetussa lausunnossa korostetaan tämän massavalvonnaksi luokiteltavan toimenpiteen olevan viimesijainen keino. Tunnistusmääräyksiä annettaisiin vain sovelluksille, joiden riski on luokiteltu korkeaksi.

Kuitenkin kun tarkastellaan keinoja, joiden ehdotuksessa katsotaan vähentävän riskiä, huomataan, että monet näistä itsessään edellyttävät massavalvontaa, eivätkä ole päästä-päähän salatuissa sovelluksissa mahdollisia toteuttaa. Lainsäätäjän ääneen lausumattomana tavoitteena on pakottaa automaattinen tunnistus käyttöön myös päästä-päähän salatuissa sovelluksissa.

Esimerkkejä tällaisista riskinhallintakeinoista, jotka eivät ole toteutettavissa sovelluksissa, joilla ei ole näkyvyyttä käyttäjien viesintään:

- sisällön moderointi
- palvelun toiminnan valvonta

- mitigaatiotoimien vaikutuksien staattinen analyysi

Ehdotuksessa myös esitetään vaihtoehtona, että mikäli käyttäjä ei hyväksy automaattisen tunnistuksen käyttöönottoa, hän ei voisi lähettää sovelluksessa kuvamateriaalia. Tällainen rajoitus tekee modernista viestintäsovelluksesta tosiasiallisesti käyttökelvottoman. Kuvamateriaalia kun voi sisältyä kuvien ja videoiden lisäksi esimerkiksi kaikkiin muihin kirjallisiin dokumentteihin: niin, Word, Excel kuin pdf-dokumentitkin voivat sisältää kuvamateriaalia. Samoin pakatut zip-tiedostot. Kuvia voidaan upottaa enkoodattuina myös puhtaaseen tekstisisältöön. Käytännössä kaikki viestit pitäisi joka tapauksessa skannata jo sen selvittämiseksi, onko niissä kuvamateriaalia vai ei.

Salatun viestintävälineen käytön tosiasiallinen kielto olisi merkittävää puuttumista sananvapauden ydinalueelle.

Ikärajat

Ikärajojen osalta pidämme tervetulleena, että nykyisessä muotoilussa on kiinnitetty huomioita käyttäjien yksityisyyden turvaamiseen. Muotoilu on nyt kuitenkin epämääräinen ja sisältää fraasin "huomioida ensisijaisesti lapsen etu". Tämän fraasin sisältöä ei esityksessä selitetä kunnolla auki. Tämä on ongelmallista, sillä lukijalle jää epäselväksi mitä muotoilu tosiasiallisesti tarkoittaa.

Lisäksi nykyinen muotoilu mahdollistaisi esimerkiksi puheenjohtajamaa Unkarissa hallinnolle kyvykkyyden valvoa mitä viestintävälineitä paikallinen oppositio ja toisinajattelijat käyttävät. Tällä tulee olemaan hyytäviä vaikutuksia jo ennestään vaarantuneelle lehdistönvapaudelle kyseisessä valtiossa.

Esityksen odotettavissa olevat käytännön seuraukset

Avaamme alla lyhyesti millaisia käytännön vaikutuksia näemme esityksellä olevan.

Ensisijaisti huomio kiinnittyy siihen räikeään yksityiskohtaan, että tämä säätely koskettaa vain keskitettyjä viestintävälineitä. Näille on tyypillistä, että viestintäväline riippuu yksittäisestä palveluntarjoajasta, johon voidaan kohdistaa oikeustoimia unionin alueella. Esimerkkejä tällaisista viestintävälineistä ovat vaikkapa WhatsApp, Signal ja Telegram.

Sen sijaan hajautetut viestintävälineet, joilla ei ole tällaista yksittäistä palveluntarjoajaa, jäävät kokonaan säätely ulkopuolelle. Esimerkkejä näistä ovat esimerkiksi anonyymiverkot, kuten Tor, ja niiden sisällä toimivat palvelut ja toisaalta muut hajautetut viestimet, kuten SimpleX tai IRC.

Ilmiselvä seuraus tästä tulee olemaan, että rikollinen toiminta siirtyy hajautettuihin viestisovelluksiin. Ongelmat lakaistaan hieman syvemmälle maton alle. Itse rikolliseen toimintaan asetus tällaisenaan ei tule juuri vaikuttamaan.

Tämä seuraus tulee nähdäksemme tapahtumaan riippumatta siitä, sisältyykö esitykseen automatisoitu viestien tunnistaminen vai ei. Rikolliset ovat herkkiä tunnistamaan riskejä ja siirtymään turvallisemmiksi kokemiinsa viestivälineisiin. Esimerkkinä tästä voidaan nähdä viimeaikainen käyttäjien massapako Telegram -palvelusta. Pelkkä Telegramin ilmoitus siitä, että aikovat tehdä jatkossa yhteistyötä viranomaisten kanssa, oli riittävä kannuste palvelun vaihtamiseen.

Ehdotetutuilla toimilla ei siis saavuteta asetuksen ensisijaista päämäärää. Näin ollen niitä ei voida pitää

tehokkaina tai välttämättöminä, eivätkä niiden aiheuttamat perusoikeuksien rajoitukset ole oikeasuhtaisia.

Toivoisimme myös, että ikärajoista huolimatta lapsille tarjottaisiin edelleen aito mahdollisuus käyttää keskitettyjä palveluita täysipainoisesti. Ei olisi esityksen tavoitteiden mukaista, jos lapsikäyttäjät siirtyisivät samoihin palveluihin kuin rikollisetkin.

Mikäli lopullinen voimaantuleva asetus tulee sisältämään nykyisen ehdotuksen merkittävät tietoturvaongelmat ja kiellettyä massavalvontaa, tulevat kaikkein luotettavimpina pidetyt avoimen lähdekoodin päästä päähän salatut viestintäsovellukset, kuten Signal ja Threema jättämään unionin. On kylläkin selvää, että kyseinen sääntely aikanaan kaatuu tuomioistuimessa lainvastaisena, mutta yksittäisten viestintäsovellusten ylläpitäjät eivät halua joutua kokemaan kyseistä oikeustaistelua.

Tällainen seuraus olisi katastrofi sananvapauden toteutumiselle unionin alueella.

Ehdotukset vaihtoehtoisiksi toimiksi

Haluamme korostaa esityksen sisältävän monia kannatettavia toimenpinteitä, joita verkkopalveluita velvoitetaan toteuttamaan näitä ovat esimerkiksi:

- käyttäjien informointi palvelun käytön riskeistä ja käyttäjien ohjaaminen luotettaviin apua tarjoaviin palveluihin
- käyttäjille tarkoitettu helppokäyttöinen ilmoitustoiminnallisuus CSAM -materiaalin havaitsemisemisesta
- prosessit reagoida ilmoituksiin tehokkaasti
- lapsikäyttäjien turvallisuuden ja CSA -materiaalin levittämisen riskien huomioiminen osana palvelun kehitystä ja valvontaa
- käyttäjien yksityisyyttä kunnioittavat oletusasetukset

Vaikka Suomen mahdollisuudet lisätä uutta sisältöä esitykseen enää tässä vaiheesa lienevät hyvin rajalliset, haluaisimme kuitenkin tuoda esille joitakin tarpeelliseksi katsomiamme toimenpiteitä, joita olisi syytä huomioida joko tässä asetuksessa tai osana jatkotoimenpiteitä:

- CSA -materiaaliin liittyvien ongelmien parempi tunnistaminen julkisisssa mielenterveyspalveluissa ja näiden palveluiden rahoituksen lisääminen
- Hyväksikäytön uhreja avustavien palveluiden rahoituksen lisääminen ylipäätään
- Anonyymien mielenterveyspalveluiden tarjoaminen CSA -materiaalia katsoville henkilöille. Parhaimman tieteellisen tutkimuksen mukaan noin puolet näistä haluaisi lopettaa materiaalin käytön. Noin puolet heistä myös pelkää, että jatkuva materiaalin katselu saattaa johtaa lapsen oikeuksien loukkaamiseen. CSA-materiaali on heille addiktio. Heille ei kuitenkaan ole tarjolla ulkopuolisia resursseja addiktion hoitamiseen.
- Rikosseuraamusten tarkastelu - esimerkiksi grooming -tyyppisen toiminnan rangaistusten koventaminen (lapsen houkutteleminen seksuaaliseen tekoon tällä hetkellä maksimissaan yksi vuosi vankeutta)
- Kansainvälisen esitutkintayhteistyön lisääminen lapsiin liittyvissä seksuaalirikostutkinnoissa. Anonyymiverkoissa epäiltyjen kanssallisuutta tai tekojen tapahtumapaikkaa on vaikea tunnistaa ja rikollinen toiminta on usein rajat ylittävää.

- Tieteellisen tutkimuksen kohdistaminen ilmiön parempaan ymmärtämiseen. Ilmiötä on tähän mennessä tutkittu hyvin vähän.

Erityisesti julkisten mielenterveyspalveluiden rahoituksen osalta huomautamme, että digitaalista nuorisotyötä ainoana suomalaisena organisaationa edistänyt Verke ajetaan tänä syksynä alas rahoituksen loputtua. https://www.verke.org/uutinen/digitaalisen-nuorisotyon-keskus-verken-toiminta-paattyy-syyyna-valtakunnallisen-rahoituksen-loppuminen/