Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

3.10.2023

Eduskunta
Suuri valiokunta

Viite: U 69/2022 vp, UJ 19/2023 vp

Lausunto: Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final)

Teknologiateollisuus sekä Kyberala kiittävät mahdollisuudesta lausua asiasta. Lausunto on Teknologiateollisuuden ja Kyberalan yhteinen. Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka tekevät puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa.

Haluamme kiinnittää huomiota seuraaviin seikkoihin:

Päästä-päähän-salaustekniikan heikentäminen vaarantaisi kyberturvallisuuden Euroopassa

Euroopan komission esitys asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä tarkoittaisi nykyisessä muodossaan päästä päähän -salaustekniikan (end-to-end-encryption, E2EE) heikentämistä sähköisten viestintäpalveluiden yhteydessä, jotta viranomaiset tai viestintäpalveluiden tarjoajat voivat skannata yksityistä viestiliikennettä. Jos ehdotus hyväksytään nykyisessä muodossaan, se luo ennennäkemättömän, perusoikeuksia loukkaavan valvontamekanismin. Heikosti salattu tieto, tai heikosti suojattu laite päätyy vääriin käsiin systemaattisesti. Jo nyt globaali tietoturvaloukkausten kustannus ylittää 10 biljoonaa euroa vuodessa.

Esityksen tavoitteena on estää ja torjua lasten seksuaalista hyväksikäyttöä, joka on tavoitteena tärkeä ja kannatettava. Komission ehdottama tapa tämän tavoitteen saavuttamiseksi olisi kuitenkin erittäin ongelmallinen ja johtaisi ojasta allikkoon. Lisäksi on ilmaantunut valitettavaa näyttöä asiantuntijoiden jo aiemmin esille nostamaan huoleen siitä, että toteutuessaan laki nostaisi uusia, edelleen laajempia vaatimuksia viranomaisten oikeudesta valvoa yksityistä viestintää. Mm. Europol on ehdottanut komission virkamiehille, että ”lain myötä perustettava EU:n asiantuntijakeskus voisi edistää muutakin kuin seksuaalisen sisällön valvontaa, sillä tästä olisi hyötyä muidenkin rikoslajien kohdalla [käännös].[1]” Julkisuuteen päätynyt pohdinta paljastaa taustalla piilevän laajemman pyrkimyksen romuttaa yksityisen sähköisen viestinnän luottamuksellisuus Euroopassa.

Päästä päähän-salaus on ihmisten ja yhteiskunnan tietoturvan peruskivi

Päästä päähän -salaus on vahvin olemassa oleva salaustekniikan käytäntö. Se on sisäänrakennettu moniin päivittäisessä elämässämme käyttämiimme viestintäsovelluksiin ja -palveluihin, myös elinkeinoelämän päivittäisiin sovelluksiin. Se on myös keskeinen osa tavallisten ihmisten tietosuojaa verkossa. Päästä päähän -salattujen sovellusten avulla käyttäjien tiedot suojataan käyttäjän omilla salausavaimilla, ja palvelimille lähetetään vain salattu versio

[1] Giacomo Zandonini, Apostolis Fotiadis and Luděk Stavinoha, BIRN. 25.9.2023. Saatavilla: https://balkaninsight.com/2023/09/25/who-benefits-inside-the-eus-fight-over-scanning-for-child-sex-content/

Eteläranta 10, PL 10, 00131 Helsinki

käyttäjien tiedoista. Tämän ansiosta palvelun ylläpitäjätkään eivät pääse käsiksi salattuun käyttäjätietoon.

Päästä päähän -salaus toimii nykyaikaisen digitaalisen infrastruktuurin ja viestinnän perustana. Vahvan päästä päähän -salauksen ylläpitäminen on olennainen perusoikeuksiemme takaamiseksi, kuten oikeuden (aineettomaan) omaisuuteen, yksityis- ja perhe-elämän kunnioittamiseen sekä sananvapauteen. Inklusiivinen ja kestävä digitaalinen talous rakentuu asianmukaiselle tietosuojan tasolle sekä kyberturvallisuudelle, joka estää rikollisuutta ja suojaa globaaleja arvo- ja toimitusketjujamme laittomalta vaikuttamiselta, vakoilulta, laittomilta tietovuodoilta ja sabotoinnilta.

On myös välttämätöntä huomata, että sekä aiemman että nykyisen komission digitaalisen turvallisuuden vahvistamispyrkimysten ja siitä seuranneiden merkittävien lakialoitteiden strateginen ydin on digitaalisen riskienhallinnan ja modernin tietoturvan ”jalkauttaminen” Eurooppaan. Lakialoitteista voidaan mainita mm. kyberturvallisuusdirektiivi (NIS2), kybersolidaarisuussäädös (CSOA), kyberturvallisuussäädöksen (CSA) päivittäminen, finanssialan digitaalinen häiriönsietokykyasetus (DORA) sekä eritoten kyberkestävyyssäädös (CRA). Yhteenvetona voidaan todeta, että lausunnon kohteena oleva lakiehdotus on muiden lakialoitteiden tietoturvallisuustavoitteiden kanssa selvässä ristiriidassa. Ristiriitaa korostaa mm. kyberkestävyyssäädöksen – joka siis koskee kaikkien Euroopan markkinoille saatettavien digitaalisen komponenttien sisältävien laitteiden ja ohjelmistojen tietoturvallisuutta – vaatimusta vahvan salauksen käyttämistä salaamalla asiaankuuluvat tiedot uusimman tekniikan mukaisilla mekanismeilla tallennustilassa tai tietojen siirron aikana.

Komission esitys tuhoaa tietosuojan

Salaustekniikan heikentäminen ei ole mahdollista ilman tietoturvallisuuden ja tietosuojan vaarantamista. Tämä johtuu siitä, että heikennetty salaustekniikka ei kestäisi pahantahtoisia yrityksiä purkaa sitä, mukaan lukien salauksenpurkutarkoituksiin alun perin jaettujen salausavainten väärinkäyttö.

Salaus ei ole pelkästään nykyaikaisen digitaalisen tiedonkäsittelyn kulmakivi, vaan myös välttämätön tekijä viestintäpalveluiden tarjonnassa, joita käyttäjät, elinkeinoelämän aikuisista lapsiin, tarvitsevat pysyäkseen verkossa turvassa. Hyväntahtoisetkin pyrkimykset tarjota laillinen salauspurkuratkaisu päästä päähän -salaustekniikalle heikentäisivät merkittävästi tietoturvahyötyjä, koska ne tekisivät kaikki tällaisten palveluiden käyttäjät haavoittuvammiksi pahantahtoisille toimille aina yksityisyysrikoksista vakoiluun.

Viranomaisille takaportin luominen elektronisten viestintäpalveluiden yhteydessä tarkoittaisi sitä, että samoja takaportteja voitaisiin käyttää myös muihin valtiollisiin, rikollisiin tai kansainvälisen oikeuden vastaisiin tarkoituksiin. Tämä heikentäisi merkittävästi digitaalista luottamusta ja toisi väistämättä samat mahdollisuudet myös rikollisten saataville. Päästä päähän -salaustekniikan heikentämisestä kärsisivät eniten tavalliset eurooppalaiset ja yritykset, joiden yksityisyyttä loukattaisiin ja jotka menettäisivät pääsyn turvallisiin viestintäpalveluihin. Rikolliset ja muut pahantahtoiset toimijat löytäisivät todennäköisesti muita tapoja kommunikoida salaisesti.

Komission esityksessä on huomattavia oikeudellisia ja perustuslaillisia ongelmia

Ehdotuksesta on esitetty oikeudellisia ja perustuslaillisia huolenaiheita monissa yhteyksissä. Valtioneuvosto on aiemman valmistelutyön yhteydessä korostanut, että ehdotusluonnos ei täytä rajoittamistoimien tiukkaa tarpeellisuuden ja suhteellisuuden vaatimusta (EU:n

perusoikeuskirjan mukaisesti) Euroopan unionin tuomioistuimen oikeuskäytännön valossa. Komission Sääntelyntarkastuslautakunta on päätynyt samoihin johtopäätöksiin (15.02.2022 SEC(2022) 209):

> *”The report is not sufficiently clear on how the options that include the detection of new child sexual abuse material or grooming would respect the prohibition of general monitoring obligations.”*

Lisäksi EU:n neuvoston oikeudellinen palvelu (8787/23) on huomauttanut samoista ongelmista, joista alla tiivistävä lainaus:

> *”…Given its general and indiscriminate nature, such screening obligation would, therefore, entail a particularly serious interference with fundamental rights.”*
>
> *“…In the light of this case law, and taking into account the considerations referred to in paragraphs 39 to 47 above, there is a serious risk of non-compliance with the principle of proportionality in so far as the detection orders would require the general and indiscriminate access to the content of personal communications by a specific service provider, and would apply without any distinction to all the persons using that specific service, without those persons being, even indirectly, in a situation liable to give rise to criminal prosecution.”*
>
> ”… Regulation with regard to interpersonal communications, constitutes a particularly serious limitation to the rights to privacy and personal data protection enshrined in Article 7 and 8 of the Charter.”
>
> “…Regulation should provide more detailed and substantive elements with respect to the technology to be used and the extent of limitations to fundamental rights that it could entail, as well as further precisions concerning the conditions for issuance of a detection order and related possible safeguard measures.”

Euroopan parlamentin omassa vaikutusarviossa (Ex-Ante Impact Assessment Unit PE 740.248 – April 2023) todetaan:

> *”The fact that the proposal targets known content, new content, and grooming, while the technologies to detect new content and grooming are of low accuracy (compared to the technologies to detect known CSAM). A majority of experts consulted consider that deploying the technologies to detect new CSAM and grooming will result in an increase in reported content and a reduction in accuracy, thereby substantially impacting law enforcement agencies' (LEAs) workload. The feasibility of the role of an EU centre in filtering reported content specifically to alleviate the burden on LEAs is questioned.”*
>
> *”The detection of CSAM in end-to-end encryption (E2EE) raises fundamental issues with regards to the secure nature of E2EE, as it creates vulnerabilities for users of E2EE communication channels.”*

Lisäksi EU:n tietosuojalautakunta ja -valtuutettu toteavat seuraavaa (EDPB-EDPS Joint Opinion 04/2022):

> *”… While the EDPB and EDPS welcome the Commission’s efforts to ensure effective action against child sexual abuse online, they consider that the Proposal raises serious*

data protection and privacy concerns. Therefore, the EDPB and EDPS would invite the co-legislators to amend the proposed Regulation, in particular to ensure that the envisaged detection obligations meet the applicable necessity and proportionality standards and do not result in the weakening or degrading of encryption on a general level."

Vahva salaustekniikka on olennainen osa luottamuksen tarjoamista ja ylläpitämistä digitaalisiin palveluihin ja järjestelmiin. Kehittäessään politiikkaa lapsiin kohdistuvan seksuaalisen hyväksikäytön torjumiseksi päättäjien ei tulisi pyrkiä heikentämään päästä päähän -salausta, vaan keskittyä siihen, miten lapset voidaan pitää tehokkaasti turvassa säilyttäen muut perusoikeudet. Lopulliseen asetukseen tulisi sisällyttää selkeä kanta, jossa ei vaadita päästä päähän -salaustekniikan heikentämistä. Maailmanlaajuinen ja erityisesti länsimainen suuntaus on salauksen vahvistaminen entisestään nopeasti kehittyvän kvanttiuhan vuoksi. Käytännössä nykyisetkin vahvan salauksen ratkaisut on uudistettava vahvemmiksi lähivuosien aikana. Salauksen heikentäminen miltään osin vaarantaisi Euroopan strategisen turvallisuuden.

Teknologiateollisuus ry

Matti Mannonen
Johtaja, Uudistuva teollisuus

Kyberala ry

Peter Sund
Toimitusjohtaja

Lisätiedot:

Peter Sund, 050 565 0621
peter.sund@teknlogiateollisuus.fi

Risto Rajala 040 5156187
risto.rajala@teknologiateollisuus.fi