Analyysi · 16. toukokuuta 2026

← Edellinen·Seuraava →

Salaus ei ole sama kuin yksityisyys: mitä metatiedot kertovat sinusta

Salattu sisältö ja näkyvät metatiedot ovat kaksi eri asiaa. Kun palvelu puhuu "päästä päähän -salauksesta", se kertoo vain puolet totuudesta.

Lukko, joka ei suojaa kaikkea

Suuri osa nykyisistä viestintäpalveluista mainostaa päästä päähän -salausta. Ja se on totta: viestien sisältö matkaa salattuna niin, ettei kukaan matkan varrella – ei edes palveluntarjoaja – voi lukea tekstiä sen ollessa siirrossa. Tähän asti väite on täsmällinen.

Ongelmana on, että sisältö on vain osa totuutta. Vaikka kukaan ei voi lukea mitä sanot, palvelu tietää muita asioita erittäin tarkasti: kenen kanssa puhut, mihin aikaan, kuinka usein, mistä likimääräisestä sijainnista, millä laitteella, kuinka monta viestiä lähetät ja vastaanotat, kuinka monta tiedostoa jaat. Tätä kaikkea kutsutaan metatiedoksi. Ja metatiedot kertovat monissa tapauksissa lähes yhtä paljon kuin itse viesti.

Mitä metatiedot paljastavat

Viestiä ei tarvitse lukea tietääkseen monia asioita. Jos henkilö soittaa tai kirjoittaa onkologille joka tiistai-aamu kello yhdeksän kuuden kuukauden ajan, keskustelua ei tarvitse kuulla arvatakseen, mitä on meneillään. Jos kaksi henkilöä vaihtaa sata viestiä päivässä ja yhtäkkiä lopettaa, viestejä ei tarvitse lukea ymmärtääkseen, mitä on tapahtunut. Jos veroasiantuntija saa kaksikymmentä viestiä peräkkäin samalta asiakkaalta neljännesvuosittaisen tilinpäätöksen aattona, viestintämalli puhuu puolestaan.

Metatiedot paljastavat käyttäytymismalleja: kuka on tekemisissä kenen kanssa, millaiset aikataulut kullakin on, milloin he ovat valveilla, milloin he nukkuvat, milloin he matkustavat, ketkä asiakkaat ovat aktiivisimpia, mitkä ammatilliset suhteet ovat tiiviimpiä. Metatietoja keräävä palvelin voi rakentaa yksityiskohtaisen profiilin kenen tahansa käyttäjän henkilökohtaisesta ja ammatillisesta elämästä lukematta koskaan sanaakaan siitä, mitä hän kirjoittaa.

On olemassa historiallinen esimerkki, joka havainnollistaa tätä karusti. NSA:n entinen johtaja Michael Hayden muotoili asian suoraan vuonna 2014: *"We kill people based on metadata"*. Väite viittasi Yhdysvaltain sotilasoperaatioihin kohteita vastaan, jotka tunnistettiin pelkästään heidän viestintämalliensa perusteella. Ei yhtäkään luettua viestiä. Vain kontaktiverkosto ja aikataulut.

Se, että palvelu kerää metatietoja, ei välttämättä tarkoita, että se käyttäisi niitä käyttäjiään vastaan. Se tarkoittaa, että sillä on kyky tehdä niin, ja että kolmannella osapuolella, jolla on pääsy näihin tietoihin – oikeuden määräyksellä, tietoturvaloukkauksen kautta tai myymällä tiedot kolmansille osapuolille, jos palveluehdot sen sallivat – on myös tämä kyky.

Pääsy yhteystietoihin

Toinen vektori, joka jää lähes huomaamatta: yhteystietoluettelo. Suuri osa viestintäpalveluista pyytää pääsyä puhelimen yhteystietoihin rekisteröitymisen yhteydessä. Ne lataavat kaikki numerot palvelimelleen näyttääkseen, kuka muu käyttää palvelua. Siitä hetkestä lähtien yrityksellä on täydellinen kartta käyttäjän suhteista, vaikka tämä ei olisi koskaan kirjoittanut yhtäkään viestiä kenellekään.

Ammatissaan vaitiolovelvolliselle – asianajajalle, lääkärille, psykologille, konsultille – tuo luettelo sisältää asiakkaita. Jos yhteystiedot on ladattu kolmannen osapuolen palvelimelle, asiakkaiden nimet ovat infrastruktuurissa, jonka lainkäyttövaltaa ja käytäntöjä ammattilainen ei hallitse. Ammattisalaisuus ei murru sinä päivänä, kun joku vuotaa keskustelun: se murtui jo paljon aiemmin, siinä hetkessä kun lataus hyväksyttiin.

Ero salaamisen ja keräämättä jättämisen välillä

Salaaminen on sisällön suojaamista. Yksityisyys on sitä, ettei kerätä sellaista, mitä ei tarvita. Ne ovat eri asioita, ja ero on toiminnallisesti kriittinen. Palvelu voi salata kaikki viestit täydellisesti ja samalla tietää lähes kaiken käyttäjistään metatietojen kautta. Nämä kaksi asiaa ovat täysin yhteensopivia. Itse asiassa se on alan hallitseva liiketoimintamalli.

Oikea kysymys palvelun todellisen yksityisyyden arvioimiseksi ei ole *"salaako se sisällön?"*. Siihen on vastattu jo vuosia sitten. Oikea kysymys on: *"mitä metatietoja se luo ja missä niitä säilytetään?"*. Ja ennen kaikkea: *"mitä metatietoja sen ei tarvitse luoda?"*.

Arkkitehtuuri, joka minimoi metatiedot rakenteellisesti – ei lupauksilla, ei sisäisillä käytännöillä – on rakenteellisesti yksityisempi kuin arkkitehtuuri, joka kerää ja salaa ne. Sillä tietoja, joita ei ole olemassa, ei voida vuotaa, myydä, luovuttaa oikeuden määräyksellä eikä menettää tietomurrossa.

Ammatilliselle lukijalle

Jos ammattitoimintaasi liittyy salassapito, luottamuksellisuus tai yksinkertaisesti kunnioitus kolmansien osapuolten tietoja kohtaan, kysymykset kannattaa esittää tässä järjestyksessä:

1. Salaako käyttämäni viestintäsovellus sisällön? (Todennäköisesti kyllä.)
2. Salaako se metatiedot? (Todennäköisesti ei.)
3. Luoko se metatietoja, joita se *ei tarvitse* toimiakseen? (Lähes varmasti kyllä.)
4. Missä näitä metatietoja säilytetään ja minkä lainkäyttövallan alla? (Todennäköisesti Euroopan talousalueen ulkopuolella.)
5. Tietääkö asiakkaani tai potilaani, että hänen tietonsa ovat siellä?

Viimeinen kysymys on se epämiellyttävä. Sillä rehellinen vastaus on useimmissa tapauksissa: ei.

Tämä artikkeli on ensimmäinen sarjassa, joka käsittelee ammatillisten viestintätyökalujen todellista toimintaa. Seuraavissa osissa käsitellään GDPR-vaatimustenmukaisuutta viestinnässä ja ammattisalaisuuden käsitettä digitaalisella aikakaudella.

Lähteet ja lisälukemista

- Hayden, M. – Puheenvuoro Johns Hopkinsin yliopistossa, 2014 ("We kill people based on metadata"). Julkiset tekstitykset saatavilla.
- GDPR (EU:n asetus 2016/679), 4 ja 5 artikla – henkilötietojen määritelmä ja käsittelyperiaatteet (metatiedot ovat henkilötietoja).
- EDPS ja EDPB – lausunnot liikenne- ja metatietojen käsittelystä sähköisessä viestinnässä (ePrivacy-direktiivi).

← EdellinenSinettivahan lyhyt historiaSeuraava →Ammattisalaisuus digitaalisella aikakaudella

Viimeaikaiset lukemiset

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ota tämä artikkeli mukaasi minne tarvitset.

↓ Markdown ↓ Pelkkä teksti ↓ PDF

Tiedosto ladataan laitteellesi. Voit tallentaa sen, tuoda sen Solo2-sovellukseen tai jakaa sen haluamallasi tavalla. Cuadernos ei päätä tiedoston kohtaloa puolestasi.

Sinetti · SHA-256 4e0cbe45aba85917e076184ed52389c994470eb25f65a5ffeececbce0df2535c

Cuadernos Lacre · Menzuri Gestión S.L. -julkaisu ·
kirjoittanut R.Eugenio · toimittanut Solo2-tiimi.