Analyysi · 16. toukokuuta 2026

← Edellinen·Seuraava →

Kun välissä ei ole ketään

Palvelimen kautta kulkevan tiedon salaaminen suojaa sisältöä. Palvelimen puuttuminen väliltä poistaa koko kysymyksen. Ne eivät ole sama asia.

Kaksi ihmistä, yksi keskustelu

Kun kaksi ihmistä puhuu kasvotusten huoneessa, kenenkään ei tarvitse luvata, ettei kuullut mitään. Hän ei kuullut, koska hän ei ollut paikalla. Kun kaksi ihmistä ojentaa paperin kädestä käteen, kenenkään välissä olevan ei tarvitse vannoa, ettei lukenut sitä. Välissä ei ole ketään.

Suurin osa asioista arkielämässä toimii näin. Emme allekirjoita salassapitosopimuksia ääntämme välittävän ilman tai kädessämme olevan paperin kanssa. Keskustelun yksityisyys ei perustu välittäjän lupaukseen, koska välittäjää ei ole. Se on yksi vahvimmista tavoista olla yksityinen: ei siksi, että jokin tai joku toimii hyvin, vaan siksi, ettei jotakin tai jotakuta ole.

Kun keskustelu siirtyy digitaaliseen kanavaan, tämä muuttuu oletusarvoisesti. Tavallinen malli on seuraava: kaksi ihmistä ottaa yhteyden palvelimeen, palvelin vastaanottaa viestin, salaa sen tai säilyttää sen salattuna ja toimittaa sen vastaanottajalle. Palvelin on välissä. Palvelin voi olla rehellinen. Se voi olla auditoitu. Se voi toimia suotuisalla lainkäyttöalueella ja tiukan tietosuojakäytännön alaisena. Kaikki tämä voi olla totta. Mutta palvelin on välissä.

Salaamisen ja keräämättä jättämisen ero (toinen osa)

Tämän sarjan aiemmassa artikkelissa väitimme, että sisällön salaaminen ja metatietojen keräämättä jättäminen eivät ole sama asia. On vielä yksi askel, joka on syytä muotoilla selkeästi: palvelimen kautta kulkevan tiedon salaaminen ja palvelimen puuttuminen eivät myöskään ole sama asia.

Ensimmäinen malli — palvelin välissä, sisältö salattuna — suojaa sisältöä palvelimen ylläpitäjältä, sen huoltohenkilöstöltä tai ulkopuoliselta hyökkääjältä, joka vaarantaa järjestelmän. Ja se on tärkeää. Mutta se ei poista palvelinta. Palvelin on edelleen siellä. Se käsittelee edelleen metatietoja. Se on edelleen piste, joka voi vastaanottaa oikeuden määräyksen, laillisen toimenpiteen, poliittista painostusta tai tietoturvaloukkauksen. Se on edelleen piste, joka edellyttää luottamusta johonkin.

Toinen malli — palvelimen puuttuminen päätepisteiden väliltä — ei suojaa salattua sisältöä paremmin: jos kryptografia on vahvaa, sisältö on suojattu kummassakin tapauksessa. Sisältö ei muutu. Se mikä muuttuu, on se, että kysymys *«mitä palvelimelle tapahtuu?»* menettää merkityksensä, koska ei ole palvelinta, josta kysyä.

Luottamus, puuttuminen ja niiden välinen ero

Luottamus voi olla hyvin ansaittua. Rehellisiä yrityksiä on olemassa. Tiukkoja tarkastajia on olemassa. Käyttäjäystävällistä lainsäädäntöä on olemassa. Vakavasti otettavia palveluita, jotka noudattavat tunnollisesti

kaikkea edellä mainittua, on olemassa. Luottamus, kun se annetaan sen ansaitsevalle operaattorille, ei ole huono järjestely.

Mutta luottamus, olipa se kuinka vahvaa tahansa, on silti luottamusta. Se on sosiaalinen ratkaisu, ei tekninen ratkaisu. Yritys voi vaihtaa omistajaa. Lainkäyttöalueen hallinto voi vaihtua. Oikeuden määräys voi tulla huomenna. Uusi haavoittuvuus voi löytyä ensi kuussa. Mikään näistä ei tapahdu pahassa tahdossa. Se tapahtuu, koska operaattori on olemassa, ja kaikki mikä on olemassa, on alttiina maailman sattumille.

Operaattorin puuttuminen ei ole näiden sattumien alainen. Oikeuden määräys ei voi pyytää tietoja palvelimelta, jota ei ole olemassa. Hyökkääjä ei voi vaarantaa palvelinta, jota ei ole olemassa. Yrityksen politiikan muutos ei voi vaikuttaa tietoihin, joita kyseisellä yrityksellä ei koskaan ollut. Avainlause on yksinkertainen: tietoja, joita ei ole olemassa, ei voi menettää.

Palvelinpuolen oikeutetusta argumentista

Ammattimaisen viestintäpalvelun tarjoaja, jolla on palvelin välissä, esittää yleensä kolme täysin pätevää argumenttia. Ensinnäkin, että palvelin on tarpeen toimituksen takaamiseksi, kun vastaanottaja on offline-tilassa. Toiseksi, että sisällön salaus on vahva, eikä operaattori siten voi lukea sitä. Kolmanneksi, että palvelu noudattaa Euroopan lainsäädäntöä ja että tiedot ovat lain suojaamia.

Kaikki kolme argumenttia ovat tosia. Mikään niistä ei muuta asian luonnetta. On totta, että palvelin mahdollistaa viestien tallentamisen myöhempää toimitusta varten; on myös totta, että viivästynyt toimitus voidaan ratkaista toisella tavalla, laitteiden välisillä suorilla viestintäprotokollilla, joita on hiottu vuosikymmeniä ja jotka ovat käytössä tänään. On totta, että sisällön salaus kuljetuksen aikana on vahvaa vakavasti otettavissa palveluissa. Ja on totta, että Euroopan lainsäädäntö suojaa käyttäjiä enemmän kuin monissa muissa paikoissa.

Kyse ei ole siitä, ovatko palvelimen sisältävät palvelut laillisia, tai ovatko ne turvallisia, tai suojaavatko ne sisältöä. Ne voivat olla niitä, ne ovat laillisia ja ne ovat yleensä turvallisia. Kyse on siitä, että palvelimen pitäminen välissä on arkkitehtoninen valinta, ei tekninen pakko. Ja jokaisella valinnalla on seurauksensa. Arkkitehtuuri, jossa on palvelin välissä, luo välttämättä toimijan, johon on luotettava. Arkkitehtuuri ilman palvelinta välissä ei.

Mitä laki sanoo ja mitä arkkitehtuuri tekee

GDPR ei edellytä tiettyä arkkitehtonista mallia. Se edellyttää tuloksia: tietojen minimointia, rajoitettua tarkoitusta, sisäänrakennettua ja oletusarvoista tietosuojaa, kykyä osoittaa vaatimustenmukaisuus. Palvelu, jossa on palvelin välissä, voi täyttää kaikki nämä vaatimukset. Palvelu ilman palvelinta välissä täyttää useita niistä rakenteellisesti, ei ilmoituksen perusteella. Absoluuttinen minimointi — eli ei kerätä mitään, mikä ei ole ehdottoman välttämätöntä viestin toimittamiseksi — on triviaalia, kun ei ole palvelinta, joka voisi kerätä jotain.

Tavalliseen, ei-arkaluonteiseen käyttöön arkkitehtuuri palvelimella on täysin kohtuullinen, ja luottamus vakavasti otettavaan operaattoriin on pätevä järjestely. Muihin käyttötarkoituksiin — niihin, joihin liittyy lakisääteinen ammattisalaisuus, joihin liittyy eettinen vastuu tai jotka koskevat erityisen arkaluonteisia tietoja — luottamuspisteen puuttuminen ei ole ylellisyyttä, vaan rakenteellinen etu.

Ammatilliselle lukijalle

Kysymykset, joita on syytä kysyä ammattimaiselta viestintäpalvelulta ja jotka ovat tuttuja tämän sarjan aiemmista artikkeleista, täydentyvät vielä yhdellä arkkitehtonisella kysymyksellä:

1. Salaako se sisällön kuljetuksen aikana? (Todennäköisesti kyllä.)
2. Luoko ja tallentaako se metatietoja siitä, kenen kanssa puhun ja milloin? (Todennäköisesti kyllä.)
3. Onko laitteeni ja vastaanottajan laitteen välisellä reitillä palvelinta?

4. Jos sellainen on: kuka sitä ylläpitää, millä lainkäyttöalueella ja mitä pitäisi tapahtua, jotta se luovuttaisi tietoja minusta?
5. Jos sellaista ei ole: edellisillä kysymyksillä ei ole merkitystä.

Näiden kahden kategorian välinen ero ei ole aste-ero, vaan tyyppiero. Kun on aika selittää se asiakkaalle, potilaalle tai kollegalle, rehellisin muotoilu on myös yksinkertaisin: toisessa on joku välissä; toisessa ei.

Tämä artikkeli päättää Cuadernos Lacre -sarjan ensimmäisen osan. Puhuttuamme salauksesta, metatiedoista ja ammattisalaisuudesta, täydennämme arkkitehtonisen kuvan: sisällön salaaminen ja palvelimen puuttuminen väliltä ovat eri asioita. Molemmat voivat olla laillisia; vain toinen poistaa luottamuspisteen.

Lähteet ja lisälukemista

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Perusteksti periaatteesta, jonka mukaan järjestelmän takuut on toteutettava päissä, ei välikanavassa.
- Asetus (EU) 2016/679, art. 25 — sisäänrakennettu ja oletusarvoinen tietosuoja.
- Asetus (EU) 2016/679, art. 5.1.c — tietojen minimoinnin periaate.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Luvut arkkitehtuureista, jotka minimoivat tiedonkeruun rakenteellisesti.

← EdellinenGDPR ja ammatillinen viestintä: miksi useimmat rikkovat sääntöjä tietämättäänSeuraava →CUADERNOS_LIST_SCHREMS_TITLE

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 8dd43bad29289d3a2b41ddd1206d95e746b65da715c43e8d57a41d9a34e21e0f

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