Analüüs · 16. mai 2026

← Eelmine·Järgmine →

Kui kedagi ei ole vahel

Läbi serveri mineva info krüpteerimine kaitseb sisu. Kui serverit vahel pole, langeb see küsimus ära. Need ei ole üks ja seesama.

Kaks inimest, üks vestlus

Kui kaks inimest räägivad ruumis näost näkku, ei pea keegi lubama, et ta ei kuulnud midagi. Ta ei kuulnud, sest teda polnud seal. Kui kaks inimest annavad teineteisele paberitükki, ei pea keegi vahepeal vanduma, et ta seda ei lugenud. Vahepeal pole kedagi.

Enamik asju igapäevaelus toimib nii. Me ei sõlmi konfidentsiaalsuslepinguid õhuga, mis edastab meie häält, ega paberiga, mida me käes hoiame. Vestluse privaatsus ei tugine vahendaja lubadusele, sest vahendajat pole. See on üks tugevamaid viise privaatsuse tagamiseks: mitte sellepärast, et miski või keegi käitub hästi, vaid sellepärast, et midagi või kedagi pole.

Kui vestlus kolib digitaalsesse kanalisse, muutub see vaikimisi. Tavaline mudel on järgmine: kaks inimest ühenduvad serveriga, server võtab sõnumi vastu, krüpteerib selle või salvestab selle krüpteeritult ning edastab saajale. Server on keskel. Server võib olla aus. See võib olla auditeeritud. See võib tegutseda soodsas jurisdiktsioonis ja range privaatsuspoliitika alusel. Kõik see võib tõsi olla. Kuid server on keskel.

Erinevus krüpteerimise ja mitte kogumise vahel (teine osa)

Eelmises sama sarja artiklis väidame, et sisu krüpteerimine ja metaandmete mitte kogumine ei ole üks ja seesama. On veel üks samm, mis tuleks selgelt välja öelda: läbi serveri mineva info krüpteerimine ja serveri puudumine pole samuti üks ja seesama.

Esimene mudel – server keskel, krüpteeritud sisu – kaitseb sisu serveri operaatori, hoolduspersonali ja süsteemi kompromiteeriva välise ründaja eest. Ja see on oluline. Kuid see ei kaota serverit. Server on endiselt seal. See töötleb endiselt metaandmeid. See jääb punktiks, mis võib saada kohtukutse, seadusliku sekkumise, poliitilise surve või turvarikkumise osaliseks. See jääb punktiks, mis nõuab kellegi usaldamist.

Teine mudel – serverit kahe otsa vahel ei ole – ei kaitse krüpteeritud sisu paremini: kui krüptograafia on kindel, on sisu mõlemal juhul kaitstud. See, mis muutub, pole sisu. Muutub see, et küsimus *"aga kuidas on serveriga?"* kaotab mõtte, sest pole serverit, mille kohta küsida.

Usaldus, puudumine ja erinevus nende kahe vahel

Usaldus võib olla õigustatud. Ausad ettevõtted eksisteerivad. Ranged audiitorid eksisteerivad. Kasutajasõbralikud seadused eksisteerivad. Tõsised teenused, mis järgivad rangelt kõike eelnevat, eksisteerivad. Usaldus, kui see on antud seda väärivale operaatorile, pole halb lahendus.

Kuid usaldus, olgu see nii kindel kui tahes, jääb usalduseks. See on sotsiaalne lahendus, mitte tehniline. Ettevõte võib omanikku vahetada. Jurisdiktsioon võib valitsust vahetada. Kohtuotsus võib saabuda homme. Järgmisel kuul võidakse avastada uus haavatavus. Midagi sellest ei juhtu pahauskselt. See juhtub, kuna operaator on olemas ja kõik olemasolev allub maailma juhustele.

Operaatori puudumine ei allu samadele juhustele. Kohtuotsus ei saa nõuda andmeid serverilt, mida pole olemas. Ründaja ei saa kompromiteerida serverit, mida pole olemas. Ettevõtte poliitika muutus ei saa mõjutada andmeid, mida ettevõttel kunagi polnud. Võtmefraas on lihtne: andmeid, mida pole olemas, ei saa kaotada.

Legitiimsest argumendist serveri poolel

See, kes pakub professionaalset sõnumsideteenust koos vahepealse serveriga, esitab tavaliselt kolm täiesti kehtivat argumenti. Esiteks, et server on vajalik kohaletoimetamise tagamiseks, kui saaja on võrguühenduseta. Teiseks, et sisu krüpteerimine on tugev ja seetõttu ei saa operaator seda lugeda. Kolmandaks, et teenus vastab Euroopa seadusandlusele ja andmed on seadusega kaitstud.

Kõik kolm argumenti on tõesed. Ükski ei muuda asja olemust. On tõsi, et server võimaldab sõnumite salvestamist hilisemaks kohaletoimetamiseks; samuti on tõsi, et hilinenud kohaletoimetamist saab lahendada teisel viisil, läbi aastakümneid viimistletud ja täna toimivate seadmetevaheliste otsesuhtlusprotokollide. On tõsi, et edastatava sisu krüpteerimine on tõsistes teenustes tugev. Ja on tõsi, et Euroopa seadusandlus kaitseb kasutajaid rohkem kui paljudes teistes kohtades.

Küsimus pole selles, kas serveriga teenused on seaduslikud, ega selles, kas need on turvalised, ega selles, kas need kaitsevad sisu. Need võivad olla, need on seaduslikud ja need on tavaliselt turvalised. Küsimus on selles, et serveri olemasolu vahepeal on arhitektuurne valik, mitte tehniline sund. Ja igal valikul on tagajärjed. Vahepealse serveriga arhitektuur loob paratamatult osaleja, keda tuleb usaldada. Arhitektuur ilma vahepealse serverita ei loo.

Mida ütleb seadus ja mida teeb arhitektuur

IKÜM ei nõua konkreetset arhitektuurimudelit. See nõuab tulemusi: andmete minimeerimist, eesmärgi piiramist, andmekaitset lõimimise ja vaikimisi, suutlikkust tõendada vastavust. Vahepealse serveriga teenus võib täita kõiki neid nõudeid. Ilma vahepealse serverita teenus täidab mitmeid neist konstruktsiooni, mitte deklaratsiooni kaudu. Absoluutne minimeerimine – ei koguta midagi, mis pole sõnumi kohaletoimetamiseks hädavajalik – on triviaalne, kui pole serverit, mis saaks midagi koguda.

Mittetundlikuks igapäevaseks kasutamiseks on serveriarhitektuur täiesti mõistlik ja usaldus tõsise operaatori vastu on kehtiv kokkulepe. Muudeks kasutusteks – neile, mis hõlmavad reguleeritud ametisaladust, eetilist vastutust või puudutavad eriti tundlikku teavet – pole usalduspunkti puudumine luksus, see on struktuurne eelis.

Professionaalsele lugejale

Küsimused, mida tuleks professionaalsele sideteenusele esitada, mis on juba tuttavad selle sarja eelmistest artiklitest, täienevad vaid ühe arhitektuurse küsimusega:

1. Kas see krüpteerib sisu edastamise ajal? (Tõenäoliselt jah.)
2. Kas see loob ja salvestab metaandmeid selle kohta, kellega ja millal ma räägin? (Tõenäoliselt jah.)
3. Kas minu seadme ja saaja vahelisel teel on server?
4. Kui see on olemas: kes seda haldab, millises jurisdiktsioonis ja mis peaks juhtuma, et nad annaksid minu kohta andmeid?
5. Kui seda ei eksisteeri: eelmised küsimused on asjakohatud.

Erinevus kahe kategooria vahel ei seisne astmes, vaid liigis. Kui tuleb aeg seda kliendile, patsiendile või kolleegile selgitada, on kõige ausam sõnastus ka kõige lihtsam: ühes on keegi vahepeal, teises ei ole.

See artikkel lõpetab Cuadernos Lacre esialgse tsükli. Pärast krüpteerimisest, metaandmetest ja ametisaladusest rääkimist täiendame arhitektuurset pilti: sisu krüpteerimine ja vahepealse serveri puudumine on erinevad asjad. Mõlemad võivad olla seaduslikud; ainult üks neist välistab usalduspunkti.

Allikad ja täiendav lugemine

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Põhitekst põhimõttele, mille kohaselt peavad süsteemi garantiid olema realiseeritud otstes, mitte vahekanalis.
- Määrus (EL) 2016/679, art. 25 — lõimitud ja vaikimisi andmekaitse.
- Määrus (EL) 2016/679, art. 5.1.c — andmete minimeerimise põhimõte.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Peatükid arhitektuuride kohta, mis minimeerivad kogumist konstruktsiooni kaudu.

← EelmineGDPR ja professionaalne sõnumside: miks enamik rikub reegleid seda teadmataJärgmine →CUADERNOS_LIST_SCHREMS_TITLE

Viimased lugemised

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 0575ed14050a8aee73222557eaf0bdcf1fdf08b26c1b2c442679131c739cc729

Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.