Anàlisi · 16 de maig de 2026

← Anterior·Següent →

Quan no hi ha ningú al mig

Xifrar el que passa per un servidor protegeix el contingut. No tenir servidor al mig elimina la pregunta. No són el mateix.

Dues persones, una conversa

Quan dues persones parlen cara a cara en una habitació, ningú ha de prometre que no ha sentit res. No ho ha sentit perquè no hi era. Quan dues persones es passen un paper d'una mà a l'altra, ningú al mig ha de jurar que no l'ha llegit. No hi ha ningú al mig.

La major part de les coses en la vida quotidiana funcionen així. No signem acords de confidencialitat amb l'aire que transmet la nostra veu, ni amb el paper que sostenim. La privadesa de la conversa no descansa sobre la promesa d'un intermediari, perquè no hi ha intermediari. Aquesta és una de les formes més fortes que existeix de ser privat: no perquè alguna cosa o algú es comporti bé, sinó perquè no hi ha res ni ningú.

Quan la conversa es trasllada a un canal digital, això canvia per defecte. El model habitual és el següent: dues persones es connecten a un servidor, el servidor rep el missatge, el xifra o el guarda xifrat, i el lliura al destinatari. El servidor està al mig. El servidor pot ser honest. Pot estar auditat. Pot operar en una jurisdicció favorable i sota una política de privadesa estricta. Tot això pot ser cert. Però el servidor està al mig.

La diferència entre xifrar i no recollir (segona part)

En un article anterior d'aquesta mateixa sèrie sostenim que xifrar el contingut i no recollir metadades no són el mateix. Hi ha un pas més enllà que convé formular amb claredat: xifrar el que passa per un servidor i no tenir servidor tampoc són el mateix.

El primer model —servidor al mig, contingut xifrat— protegeix el contingut de l'operador del servidor, del seu personal de manteniment, d'un atacant extern que comprometi el sistema. I això és important. Però no elimina al servidor. El servidor continua allí. Continua processant metadades. Continua sent un punt que pot rebre un requeriment judicial, una intervenció legal, una pressió política, o una bretxa de seguretat. Continua sent un punt que requereix dipositar confiança en algú.

El segon model —no haver-hi servidor entre els dos extrems— no protegeix millor el contingut xifrat: si la criptografia és sòlida, el contingut va protegit en tots dos casos. El que canvia no és el contingut. El que canvia és que la pregunta *«què passa amb el servidor?»* deixa de tenir objecte, perquè no existeix servidor sobre el qual preguntar.

Confiança, absència, i la diferència entre totes dues

La confiança pot estar ben dipositada. Empreses honestes existeixen. Auditors rigorosos existeixen. Legislacions favorables a l'usuari existeixen. Serveis seriosos que compleixen escrupolosament amb tot l'anterior existeixen. La confiança, quan es concedeix a un operador que la mereix, no és un mal tracte.

Però la confiança, per sòlida que sigui, continua sent confiança. És una solució social, no una solució tècnica. Una empresa pot canviar de mans. Una jurisdicció pot canviar de govern. Una ordre judicial pot arribar demà. Una vulnerabilitat nova pot descobrir-se el mes que ve. Res d'això succeeix per mala fe. Succeeix perquè l'operador existeix, i tot el que existeix està subjecte a les contingències del món.

L'absència d'un operador no està subjecte a aquestes mateixes contingències. Una ordre judicial no pot demanar dades a un servidor que no existeix. Un atacant no pot comprometre un servidor que no existeix. Un canvi en la política d'una empresa no pot afectar dades que aquesta empresa mai va tenir. La frase clau és senzilla: les dades que no existeixen no es poden perdre.

Sobre l'argument legítim del costat del servidor

Qui ofereix un servei de missatgeria professional amb servidor al mig sol formular tres arguments perfectament vàlids. Primer, que el servidor és necessari per a garantir el lliurament quan el destinatari està desconnectat. Segon, que el xifrat del contingut es robust i, per tant, l'operador no pot llegir-lo. Tercer, que el servei compleix la legislació europea i que les dades estan protegides per la llei.

Els tres arguments són certs. Cap canvia la naturalesa de l'assumpte. És cert que un servidor permet emmagatzemar missatges per a lliurament diferit; també és cert que el lliurament diferit es pot resoldre d'una altra forma, mitjançant protocols de comunicació directa entre dispositius refinats des de fa dècades i operatius avui. És cert que el xifrat del contingut en trànsit és robust en els serveis seriosos. I és cert que la legislació europea protegeix els usuaris més que la de molts altres llocs.

La qüestió no és si els serveis amb servidor al mig són legals, ni si són segurs, ni si protegeixen el contingut. Poden ser-ho, són legals, i solen ser segurs. La qüestió és que tenir un servidor al mig és una elecció arquitectònica, no una imposició tècnica. I cada elecció té conseqüències. Una arquitectura amb servidor al mig genera necessàriament un actor en qui cal confiar. Una arquitectura sense servidor al mig no.

El que la llei diu, i el que l'arquitectura fa

El RGPD no exigeix un model arquitectònic concret. Exigeix resultats: minimització de dades, finalitat limitada, protecció des del disseny i per defecte, capacitat de demostrar el compliment. Un servei amb servidor al mig pot complir tots aquests requisits. Un servei sense servidor al mig compleix diversos d'ells per construcció, no per declaració. La minimització absoluta —no recollir res que no sigui estrictament necessari per a lliurar el missatge— és trivial quan no existeix un servidor que pugui recollir res.

Per als usos quotidians no sensibles, una arquitectura amb servidor és perfectament raonable, i la confiança en un operador seriós és un acord vàlid. Per als altres usos —els que porten secret professional reglat, els que comporten responsabilitat deontològica, els que toquen informació especialment sensible— l'absència d'un punt de confiança no és un luxe, és un avantatge estructural.

Per al lector professional

Les preguntes que convé fer-se davant un servei de comunicació professional, ja familiars d'articles anteriors en aquesta mateixa sèrie, es completen amb una sola pregunta arquitectònica més:

1. Xifra el contingut en trànsit? (Probablement sí.)
2. Genera i emmagatzema metadades sobre amb qui parlo i quan? (Probablement sí.)
3. Existeix un servidor en el camí entre el meu dispositiu i el del destinatari?
4. Si existeix: qui l'opera, en quina jurisdicció, i què hauria de passar perquè lliurés dades sobre mi?
5. Si no existeix: les preguntes anteriors no tenen objecte.

La diferència entre les dues categories no és de grau, sinó de tipus. Arribat el moment d'explicar-ho a un client, a un pacient, o a un col·lega, la formulació més honesta és també la més senzilla: en una hi ha algú al mig; en l'altra, no.

Aquest article tanca el cicle inicial de Cuadernos Lacre. Després de parlar del xifrat, les metadades i el secret professional, completem el quadre arquitectònic: xifrar el contingut i no tenir servidor al mig són coses distintes. Totes dues poden ser legals; només una elimina el punt de confiança.

Fonts i lectura addicional

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Text fundacional del principi segons el qual les garanties d'un sistema s'han d'implementar en els extrems, no en el canal intermedi.
- Reglament (UE) 2016/679, art. 25 — protecció de dades des del disseny i per defecte.
- Reglament (UE) 2016/679, art. 5.1.c — principi de minimització de dades.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capítols sobre arquitectures que minimitzen la recol·lecció per construcció.

← AnteriorRGPD i missatgeria professional: per què la majoria incompleix sense saber-hoSegüent →CUADERNOS_LIST_SCHREMS_TITLE

Lectures recents

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Emporta't aquest article on el necessitis.

↓ Markdown ↓ Text pla ↓ PDF

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 2b4840ce8979efb557db8710966a355e92dbade9a0bb5d4cae33b86de0d184eb

Cuadernos Lacre · Una publicació de Menzuri Gestión S.L. ·
escrita per R.Eugenio · editada per l'equip de Solo2.