Analiză · 16 mai 2026

← Precedent·Următor →

Când nu este nimeni la mijloc

Criptarea a ceea ce trece printr-un server protejează conținutul. Lipsa unui server la mijloc elimină întrebarea. Nu sunt același lucru.

Două persoane, o conversație

Când două persoane vorbesc față în față într-o cameră, nimeni nu trebuie să promită că nu a auzit nimic. Nu a auzit pentru că nu era acolo. Când două persoane își dau o hârtie din mână în mână, nimeni la mijloc nu trebuie să jure că nu a citit-o. Nu este nimeni la mijloc.

Cele mai multe lucruri în viața de zi cu zi funcționează astfel. Nu semnăm acorduri de confidențialitate cu aerul care ne transmite vocea, nici cu hârtia pe care o ținem în mână. Confidențialitatea conversației nu se bazează pe promisiunea unui intermediar, deoarece nu există niciun intermediar. Aceasta este una dintre cele mai puternice forme de a fi privat care există: nu pentru că ceva sau cineva se comportă bine, ci pentru că nu există ceva sau cineva.

Când conversația se mută pe un canal digital, acest lucru se schimbă implicit. Modelul obișnuit este următorul: două persoane se conectează la un server, serverul primește mesajul, îl criptează sau îl păstrează criptat și îl livrează destinatarului. Serverul este la mijloc. Serverul poate fi onest. Poate fi auditat. Poate opera într-o jurisdicție favorabilă și sub o politică de confidențialitate strictă. Toate acestea pot fi adevărate. Dar serverul este la mijloc.

Diferența dintre a cripta și a nu colecta (partea a doua)

Într-un articol anterior din această serie, susținem că a cripta conținutul și a nu colecta metadate nu sunt același lucru. Există un pas mai departe care merită formulat cu claritate: a cripta ceea ce trece printr-un server și a nu avea server nu sunt, de asemenea, același lucru.

Primul model — server la mijloc, conținut criptat — protejează conținutul de operatorul serverului, de personalul său de întreținere, de un atacator extern care ar compromite sistemul. Și acest lucru este important. Dar nu elimină serverul. Serverul rămâne acolo. Continuă să proceseze metadate. Continuă să fie un punct care poate primi o solicitare judiciară, o intervenție legală, o presiune politică sau o breșă de securitate. Continuă să fie un punct care necesită acordarea încrederii cuiva.

Al doilea model — absența unui server între cele două extremități — nu protejează mai bine conținutul criptat: dacă criptografia este solidă, conținutul este protejat în ambele cazuri. Ceea ce se schimbă nu este conținutul. Ceea ce se schimbă este faptul că întrebarea *„ce se întâmplă cu serverul?”* nu mai are obiect, deoarece nu există niciun server despre care să întrebăm.

Încrederea, absența și diferența dintre ambele

Încrederea poate fi bine acordată. Există companii oneste. Există auditori riguroşi. Există legislaţii favorabile utilizatorului. Există servicii serioase care respectă cu scrupulozitate toate cele de mai sus. Încrederea, când este acordată unui operator care o merită, nu este un aranjament rău.

Dar încrederea, oricât de solidă ar fi, rămâne încredere. Este o soluție socială, nu o soluție tehnică. O companie își poate schimba proprietarul. O jurisdicție poate schimba guvernul. Un ordin judecătoresc poate sosi mâine. O vulnerabilitate nouă poate fi descoperită luna viitoare. Nimic din toate acestea nu se întâmplă din rea-credință. Se întâmplă pentru că operatorul există, iar tot ceea ce există este supus contingențelor lumii.

Absența unui operator nu este supusă acelorași contingențe. Un ordin judecătoresc nu poate cere date unui server care nu există. Un atacator nu poate compromite un server care nu există. O schimbare în politica unei companii nu poate afecta date pe care acea companie nu le-a avut niciodată. Fraza cheie este simplă: datele care nu există nu pot fi pierdute.

Despre argumentul legitim al părții de server

Cei care oferă un serviciu de mesagerie profesională cu server la mijloc formulează de obicei trei argumente perfect valabile. Primul, că serverul este necesar pentru a garanta livrarea când destinatarul este deconectat. Al doilea, că criptarea conținutului este robustă și, prin urmare, operatorul nu îl poate citi. Al treilea, că serviciul respectă legislația europeană și că datele sunt protejate prin lege.

Toate cele trei argumente sunt adevărate. Niciunul nu schimbă natura problemei. Este adevărat că un server permite stocarea mesajelor pentru livrare amânată; este, de asemenea, adevărat că livrarea amânată poate fi rezolvată în alt mod, prin protocoale de comunicare directă între dispozitive, rafinate de decenii și operaționale astăzi. Este adevărat că criptarea conținutului în tranzit este robustă în serviciile serioase. Și este adevărat că legislația europeană protejează utilizatorii mai mult decât cea din multe alte locuri.

Problema nu este dacă serviciile cu server la mijloc sunt legale, nici dacă sunt sigure, nici dacă protejează conținutul. Pot fi, sunt legale și sunt de obicei sigure. Problema este că a avea un server la mijloc este o alegere de arhitectură, nu o impunere tehnică. Și fiecare alegere are consecințe. O arhitectură cu server la mijloc generează neapărat un actor în care trebuie să ai încredere. O arhitectură fără server la mijloc, nu.

Ce spune legea și ce face arhitectura

GDPR nu impune un anumit model arhitectural. Impune rezultate: minimizarea datelor, finalitate limitată, protecție din faza de proiectare și în mod implicit, capacitatea de a demonstra conformitatea. Un serviciu cu server la mijloc poate îndeplini toate aceste cerințe. Un serviciu fără server la mijloc îndeplinește mai multe dintre ele prin construcție, nu prin declarație. Minimizarea absolută — a nu colecta nimic din ceea ce nu este strict necesar pentru a livra mesajul — este banală când nu există un server care să poată colecta ceva.

Pentru utilizările cotidiene nesensibile, o arhitectură cu server este perfect rezonabilă, iar încrederea într-un operator serios este un aranjament valabil. Pentru celelalte utilizări — cele care implică secret profesional reglementat, cele care implică responsabilitate deontologică, cele care ating informații deosebit de sensibile — absența unui punct de încredere nu este un lux, este un avantaj structural.

Pentru cititorul profesionist

Întrebările care merită puse în fața unui serviciu de comunicare profesională, deja familiare din articolele anterioare din această serie, se completează cu o singură întrebare de arhitectură în plus:

1. Criptează conținutul în tranzit? (Probabil că da.)
2. Generează și stochează metadate despre persoana cu care vorbesc și când? (Probabil că da.)
3. Există un server pe drumul dintre dispozitivul meu și cel al destinatarului?

4. Dacă există: cine îl operează, în ce jurisdicție și ce ar trebui să se întâmple pentru ca acesta să furnizeze date despre mine?
5. Dacă nu există: întrebările anterioare nu au obiect.

Diferența dintre cele două categorii nu este de grad, ci de tip. Când vine momentul să îi explici unui client, unui pacient sau unui coleg, formularea cea mai onestă este și cea mai simplă: într-una este cineva la mijloc; în cealaltă, no.

Acest articol încheie ciclul inițial al Cuadernos Lacre. După ce am vorbit despre criptare, metadate și secretul profesional, completăm tabloul arhitectural: a cripta conținutul și a nu avea server la mijloc sunt lucruri diferite. Ambele pot fi legale; doar una elimină punctul de încredere.

Surse și lecturi suplimentare

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Textul fundamental al principiului conform căruia garanțiile unui sistem trebuie implementate la extremități, nu în canalul intermediar.
- Regulamentul (UE) 2016/679, art. 25 — protecția datelor din faza de proiectare și în mod implicit.
- Regulamentul (UE) 2016/679, art. 5.1.c — principiul minimizării datelor.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capitole despre arhitecturi care minimizează colectarea prin construcție.

← PrecedentGDPR și mesageria profesională: de ce majoritatea încalcă normele fără să știeUrmător →CUADERNOS_LIST_SCHREMS_TITLE

Lecturi recente

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Luați acest articol cu dumneavoastră oriunde aveți nevoie.

↓ Markdown ↓ Text simplu ↓ PDF

Fișierul se va descărca pe dispozitivul dumneavoastră. De acolo îl puteți salva, importa în Solo2 sau partaja oriunde doriți. Cuadernos nu decide destinația în locul dumneavoastră.

Sigiliu de ceară · SHA-256 73c45842c9bf594084736b791b854c97fead30802a38f20bb131be52129cd468

Cuadernos Lacre · O publicație a Menzuri Gestión S.L. ·
scrisă de R.Eugenio · editată de echipa Solo2.