Analys · 16 maj 2026

← Föregående·Nästa →

När ingen är emellan

Att kryptera det som passerar genom en server skyddar innehållet. Att inte ha en server emellan eliminerar frågan. De är inte samma sak.

Två personer, ett samtal

När två personer pratar ansikte mot ansikte i ett rum behöver ingen lova att de inte hörde något. De hörde inget eftersom de inte var där. När två personer räcker ett papper från hand till hand behöver ingen i mitten svära på att de inte läste det. Det finns ingen i mitten.

Det mesta i vardagen fungerar så. Vi skriver inte sekretessavtal med luften som överför vår röst, eller med papperet vi håller i. Samtalets integritet vilar inte på en mellanhands löfte, eftersom det inte finns någon mellanhand. Det är ett av de starkaste sätten att vara privat på: inte för att något eller någon beter sig bra, utan för att något eller någon inte finns.

När samtalet flyttar till en digital kanal ändras detta som standard. Den vanliga modellen är följande: två personer ansluter till en server, servern tar emot meddelandet, krypterar det eller sparar det krypterat och levererar det till mottagaren. Servern är i mitten. Servern kan vara ärlig. Den kan vara reviderad. Den kan verka i en gynnsam jurisdiktion och under en strikt integritetspolicy. Allt detta kan vara sant. Men servern är i mitten.

Skillnaden mellan att kryptera och att inte samla in (del två)

I en tidigare artikel i samma serie hävdade vi att kryptering av innehåll och att inte samla in metadata inte är samma sak. Det finns ytterligare ett steg som bör formuleras tydligt: att kryptera det som passerar genom en server och att inte ha någon server alls är inte heller samma sak.

Den första modellen — server i mitten, krypterat innehåll — skyddar innehållet från serveroperatören, dess underhållspersonal och en extern angripare som komprometterar systemet. Och det är viktigt. Men det tar inte bort servern. Servern finns kvar. Den fortsätter att behandla metadata. Den fortsätter att vara en punkt som kan ta emot ett domstolsbeslut, ett lagligt ingripande, politisk press eller ett säkerhetsintrång. Det är fortfarande en punkt som kräver att man ger sitt förtroende till någon.

Den andra modellen — att inte ha någon server mellan de två ändpunkterna — skyddar inte det krypterade innehållet bättre: om kryptografin är solid är innehållet skyddat i båda fallen. Det är inte innehållet som ändras. Det som ändras är att frågan *"vad händer med servern?"* blir irrelevant, eftersom det inte finns någon server att fråga om.

Förtroende, frånvaro och skillnaden däremellan

Förtroende kan vara välplacerat. Ärliga företag finns. Rigorösa revisorer finns. Användarvänlig lagstiftning finns. Seriösa tjänster som strikt följer allt ovanstående finns. Förtroende, när det ges till en operatör som förtjänar det, är inte en dålig lösning.

Men förtroende, hur stabilt det än är, förblir förtroende. Det är en social lösning, inte en teknisk lösning. Ett företag kan byta ägare. En jurisdiktion kan byta regering. Ett domstolsbeslut kan komma imorgon. En ny sårbarhet kan upptäckas nästa månad. Inget av detta sker av ond tro. Det händer för att operatören finns, och allt som finns är föremål för världens tillfälligheter.

Frånvaron av en operatör är inte föremål för samma tillfälligheter. Ett domstolsbeslut kan inte begära data från en server som inte finns. En angripare kan inte kompromettera en server som inte finns. En ändring i ett företags policy kan inte påverka data som företaget aldrig haft. Nyckelmeningen är enkel: data som inte finns kan inte förloras.

Om det legitima argumentet från serversidan

Den som erbjuder en professionell meddelandetjänst med en server i mitten brukar formulera tre helt giltiga argument. För det första att servern är nödvändig för att garantera leverans när mottagaren är offline. För det andra att krypteringen av innehållet är robust och att operatören därför inte kan läsa det. För det tredje att tjänsten följer europeisk lagstiftning och att data skyddas av lagen.

Alla tre argumenten är sanna. Inget ändrar sakens natur. Det är sant att en server gör det möjligt att lagra meddelanden för senare leverans; det är också sant att senare leverans kan lösas på annat sätt, genom protokoll för direkt kommunikation mellan enheter som förfinats under årtionden och är i drift idag. Det är sant att krypteringen av innehåll under överföring är robust i seriösa tjänster. Och det är sant att europeisk lagstiftning skyddar användare mer än på många andra platser.

Frågan är inte om tjänster med en server i mitten är lagliga, eller om de är säkra, eller om de skyddar innehållet. De kan vara det, de är lagliga och de är vanligtvis säkra. Frågan är att ha en server i mitten är ett arkitektoniskt val, inte ett tekniskt krav. Och varje val har konsekvenser. En arkitektur med en server i mitten skapar nödvändigtvis en aktör som man måste lita på. En arkitektur utan en server i mitten gör det inte.

Vad lagen säger och vad arkitekturen gör

GDPR kräver inte en specifik arkitektonisk modell. Den kräver resultat: dataminimering, ändamålsbegränsning, skydd genom design och som standard, förmåga att visa efterlevnad. En tjänst med en server i mitten kan uppfylla alla dessa krav. En tjänst utan en server i mitten uppfyller flera av dem genom konstruktion, inte genom deklaration. Absolut minimering — att inte samla in något som inte är strikt nödvändigt för att leverera meddelandet — är trivialt när det inte finns någon server som kan samla in något.

För vardagliga, icke-känsliga användningsområden är en serverarkitektur helt rimlig, och förtroende för en seriös operatör är en giltig lösning. För andra användningsområden — de som omfattas av reglerad tystnadsplikt, de som medför yrkesetiskt ansvar, de som rör särskilt känslig information — är frånvaron av en förtroendepunkt inte en lyx, utan en strukturell fördel.

För den professionella läsaren

Frågorna som bör ställas till en professionell kommunikationstjänst, redan bekanta från tidigare artiklar i denna serie, kompletteras med bara en arkitektonisk fråga till:

1. Krypteras innehållet under överföring? (Förmodligen ja.)
2. Skapas och lagras metadata om vem jag pratar med och när? (Förmodligen ja.)
3. Finns det en server på vägen mellan min enhet och mottagarens?
4. Om den finns: vem driver den, i vilken jurisdiktion och vad skulle krävas för att de ska lämna ut uppgifter om mig?
5. Om den inte finns: de föregående frågorna är irrelevanta.

Skillnaden mellan de två kategorierna är inte en fråga om grad, utan om typ. När det är dags att förklara det för en kund, en patient eller en kollega är den ärligaste formuleringen också den enklaste: i den ena finns det någon i mitten; i den andra, nej.

Denna artikel avslutar den inledande cykeln av Cuadernos Lacre. Efter att ha pratat om kryptering, metadata och tystnadsplikt kompletterar vi den arkitektoniska bilden: att kryptera innehållet och att inte ha en server i mitten är olika saker. Båda kan vara lagliga; bara en eliminerar förtroendepunkten.

Källor och vidare läsning

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Grundläggande text om principen att ett systems garantier bör implementeras i ändpunkterna, inte i den mellanliggande kanalen.
- Förordning (EU) 2016/679, art. 25 — dataskydd genom design och som standard.
- Förordning (EU) 2016/679, art. 5.1.c — principen om dataminimering.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitel om arkitekturer som minimerar insamling genom konstruktion.

← FöregåendeGDPR och professionell messaging: varför de flesta bryter mot reglerna utan att veta om detNästa →CUADERNOS_LIST_SCHREMS_TITLE

Senaste läsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 7b00e02f832d4c24cda5da8b439e138ccb0e3b6719607b64c527a71347449a2c

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.