Analyse · 16. mai 2026

← Forrige·Neste →

Når ingen er i midten

Å kryptere det som passerer gjennom en server beskytter innholdet. Å ikke ha en server i midten eliminerer spørsmålet. Det er ikke det samme.

To personer, én samtale

Når to personer snakker ansikt til ansikt i et rom, trenger ingen å love at de ikke hørte noe. De hørte ikke fordi de ikke var der. Når to personer gir hverandre et papir fra hånd til hånd, trenger ingen i midten å sverge på at de ikke leste det. Det er ingen i midten.

De fleste ting i hverdagen fungerer på denne måten. Vi signerer ikke taushetserklæringer med luften som overfører stemmene våre, heller ikke med papiret vi holder. Samtalens personvern hviler ikke på løftet til en mellommann, fordi det ikke finnes noen mellommann. Det er en av de sterkeste formene for å være privat som finnes: ikke fordi noe eller noen oppfører seg bra, men fordi det ikke er noe eller noen der.

Når samtalen flyttes til en digital kanal, endres dette som standard. Den vanlige modellen er som følger: to personer kobler seg til en server, serveren mottar meldingen, krypterer den eller lagrer den kryptert, og leverer den til mottakeren. Serveren er i midten. Serveren kan være ærlig. Den kan være revidert. Den kan operere i en gunstig jurisdiksjon og under en streng personvernerklæring. Alt dette kan være sant. Men serveren er i midten.

Forskjellen mellom å kryptere og ikke å samle inn (del to)

I en tidligere artikkel i denne serien hevder vi at å kryptere innholdet og ikke å samle inn metadata ikke er det samme. Det er et skritt videre som bør formuleres tydelig: å kryptere det som passerer gjennom en server og ikke å ha en server er heller ikke det samme.

Den første modellen — server i midten, kryptert innhold — beskytter innholdet fra serveroperatøren, fra vedlikeholdspersonellet, fra en ekstern angriper som kompromitterer systemet. Og det er viktig. Men det fjerner ikke serveren. Serveren er fortsatt der. Den behandler fortsatt metadata. Den er fortsatt et punkt som kan motta en rettskjennelse, et juridisk inngrep, politisk press eller et sikkerhetsbrudd. Det er fortsatt et punkt som krever at man stoler på noen.

Den andre modellen — å ikke ha en server mellom de to endene — beskytter ikke det krypterte innholdet bedre: hvis kryptografien er solid, er innholdet beskyttet i begge tilfeller. Det som endres er ikke innholdet. Det som endres er at spørsmålet *«hva skjer med serveren?»* mister sin betydning, fordi det ikke finnes noen server å spørre om.

Tillit, fravær, og forskjellen mellom dem

Tillit kan være velplassert. Ærlige selskaper eksisterer. Strenge revisorer eksisterer. Brukervennlige lover eksisterer. Seriøse tjenester som nøye overholder alt det ovennevnte eksisterer. Tillit, når den gis til en operatør som fortjener det, er ikke en dårlig ordning.

Men tillit, uansett hvor solid den er, forblir tillit. Det er en sosial løsning, ikke en teknisk løsning. Et selskap kan bytte eiere. En jurisdiksjon kan bytte regjering. En rettskjennelse kan komme i morgen. Et nytt sårbarhet kan oppdages neste måned. Ingenting av dette skjer av ond vilje. Det skjer fordi operatøren eksisterer, og alt som eksisterer er underlagt verdens tilfeldigheter.

Fraværet av en operatør er ikke underlagt disse samme tilfeldighetene. En rettskjennelse kan ikke be om data fra en server som ikke eksisterer. En angriper kan ikke kompromittere en server som ikke eksisterer. En endring i selskapets retningslinjer kan ikke påvirke data som selskapet aldri har hatt. Nøkkelfrasen er enkel: data som ikke eksisterer kan ikke gå tapt.

Om det legitime argumentet på serversiden

De som tilbyr en profesjonell meldingstjeneste med en server i midten formulerer vanligvis tre helt gyldige argumenter. For det første, at serveren er nødvendig for å garantere levering når mottakeren er frakoblet. For det andre, at krypteringen av innholdet er robust og at operatøren derfor ikke kan lese det. For det tredje, at tjenesten overholder europeisk lovgivning og at dataene er beskyttet av loven.

Alle tre argumentene er sanne. Ingen av dem endrer sakens natur. Det er sant at en server tillater lagring av meldinger for forsinket levering; det er også sant at forsinket levering kan løses på andre måter, gjennom protokoller for direkte kommunikasjon mellom enheter som har blitt forbedret i flere tiår og fungerer i dag. Det er sant at krypteringen av innholdet under overføring er robust i seriøse tjenester. Og det er sant at europeisk lovgivning beskytter brukerne bedre enn mange andre steder.

Spørsmålet er ikke om tjenestene med en server i midten er lovlige, eller om de er sikre, eller om de beskytter innholdet. De kan være det, de er lovlige, og de er vanligvis sikre. Spørsmålet er at det å ha en server i midten er et arkitektonisk valg, ikke et teknisk krav. Og hvert valg har konsekvenser. En arkitektur med en server i midten skaper uunngåelig en aktør man må stole på. En arkitektur uten en server i midten gjør ikke det.

Hva loven sier, og hva arkitekturen gjør

GDPR krever ikke en bestemt arkitektonisk modell. Den krever resultater: dataminimering, formålsbegrensning, innebygd personvern og personvern som standard, og evnen til å bevise samsvar. En tjeneste med en server i midten kan oppfylle alle disse kravene. En tjeneste uten en server i midten oppfyller flere av dem ved konstruksjon, ikke ved deklarasjon. Absolutt minimering — å ikke samle inn noe som ikke er strengt nødvendig for å levere meldingen — er trivielt når det ikke finnes en server som kan samle inn noe.

For hverdagslige og ikke-sensitive bruksområder er en arkitektur med server helt fornuftig, og tillit til en seriøs operatør er en gyldig ordning. For andre formål — de som innebærer lovpålagt taushetsplikt, de som medfører yrkesetisk ansvar, de som berører spesielt sensitiv informasjon — er fraværet av et tillitspunkt ikke en luksus, det er en strukturell fordel.

For den profesjonelle leseren

Spørsmålene man bør stille seg i møte med en profesjonell kommunikasjonstjeneste, som allerede er kjent fra tidligere artikler i denne serien, kompletteres med bare ett arkitektonisk spørsmål til:

1. Krypterer det innholdet under overføring? (Sannsynligvis ja.)
2. Genererer og lagrer det metadata om hvem jeg snakker med og når? (Sannsynligvis ja.)
3. Finnes det en server på veien mellom min enhet og mottakerens?
4. Hvis den eksisterer: hvem drifter den, i hvilken jurisdiksjon, og hva måtte ha skjedd for at de skulle utlevere data om meg?
5. Hvis den ikke eksisterer: de foregående spørsmålene er irrelevante.

Forskjellen mellom de两kategoriene er ikke en gradsforskjell, men en vesensforskjell. Når tiden er inne for å forklare det til en klient, en pasient eller en kollega, er den ærligste formuleringen også den enkleste: i den ene er det noen i midten; i den andre, ikke.

Denne artikkelen avslutter den første syklusen av Cuadernos Lacre. Etter å ha snakket om kryptering, metadata og taushetsplikt, kompletterer vi det arkitektoniske bildet: å kryptere innholdet og ikke å ha en server i midten er forskjellige ting. Begge kan være lovlige; bare én eliminerer tillitspunktet.

Kilder og videre lesing

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Grunnleggende tekst for prinsippet om at systemets garantier bør implementeres i endene, ikke i den mellomliggende kanalen.
- Forordning (EU) 2016/679, art. 25 — innebygd personvern og personvern som standard.
- Forordning (EU) 2016/679, art. 5.1.c — prinsippet om dataminimering.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitler om arkitekturer som minimerer innsamling ved design.

← ForrigeGDPR og profesjonell messaging: hvorfor de fleste bryter reglene uten å vite detNeste →CUADERNOS_LIST_SCHREMS_TITLE

Siste lesninger

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med deg denne artikkelen dit du trenger den.

↓ Markdown ↓ Klartekst ↓ PDF

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 6015dac6593fb9dbed4829f5a0cab0cd9e4b053499224f5a790d01c726bc04a0

Cuadernos Lacre · En utgivelse fra Menzuri Gestión S.L. ·
skrevet av R.Eugenio · redigert av teamet bak Solo2.