Analyse · 16. maj 2026

← Forrige·Næste →

Når der ikke er nogen imellem

Kryptering af det, der passerer gennem en server, beskytter indholdet. At der ikke er en server imellem, eliminerer spørgsmålet. Det er ikke det samme.

Two personer, én samtale

Når to personer taler ansigt til ansigt i et rum, behøver ingen at love, at de intet hørte. De hørte intet, fordi de ikke var der. Når to personer rækker et papir fra hånd til hånd, behøver ingen i midten at sværge på, at de ikke læste det. Der er ingen i midten.

De fleste ting i hverdagen fungerer på denne måde. Vi underskriver ikke fortrolighedsaftaler med den luft, der transmitterer vores stemme, eller med det papir, vi holder. Samtalens privatliv hviler ikke på et løfte fra en mellemmand, for der er ingen mellemmand. Det er en af de stærkeste former for privatliv, der findes: Ikke fordi noget eller nogen opfører sig pænt, men fordi der ikke er noget eller nogen.

Når samtalen flytter til en digital kanal, ændres dette som standard. Den sædvanlige model er følgende: To personer forbinder til en server, serveren modtager beskeden, krypterer den eller gemmer den krypteret og leverer den til modtageren. Serveren er imellem dem. Serveren kan være ærlig. Den kan være auditeret. Den kan operere i en gunstig jurisdiktion og under en streng privatlivspolitik. Alt det kan være sandt. Men serveren er imellem dem.

Forskellen mellem at kryptere og ikke at indsamle (anden del)

I en tidligere artikel i denne serie hævder vi, at kryptering af indhold og det ikke at indsamle metadata ikke er det samme. Der er et skridt videre, som det er værd at formulere klart: Kryptering af det, der passerer gennem en server, og det slet ikke at have en server, er heller ikke det samme.

Den første model — server i midten, krypteret indhold — beskytter indholdet mod serveroperatøren, vedligeholdelsespersonalet og en ekstern angriber, der kompromitterer systemet. Og det er vigtigt. Men det fjerner ikke serveren. Serveren er der stadig. Den behandler stadig metadata. Den er stadig et punkt, der kan modtage en retskendelse, et juridisk indgreb, et politisk pres eller et sikkerhedsbrud. Det er stadig et punkt, der kræver tillid til nogen.

Den anden model — ingen server mellem de to ender — beskytter ikke det krypterede indhold bedre: Hvis kryptografien er solid, er indholdet beskyttet i begge tilfælde. Det, der ændrer sig, er ikke indholdet. Det, der ændrer sig, er at spørgsmålet *«hvad med serveren?»* bliver irrelevant, fordi der ikke findes en server at spørge om.

Tillid, fravær og forskellen mellem de to

Tillid kan være velfunderet. Ærlige virksomheder findes. Omhyggelige revisorer findes. Brugerlovgivning findes. Seriøse tjenester, der samvittighedsfuldt overholder alt det ovenstående, findes. Tillid, når den gives til en

operatør, der fortjener den, er ikke en dårlig ordning.

Men tillid, uanset hvor solid den er, forbliver tillid. Det er en social løsning, ikke en teknisk løsning. En virksomhed kan skifte hænder. En jurisdiktion kan skifte regering. En retskendelse kan komme i morgen. En ny sårbarhed kan blive opdaget i næste måned. Intet af dette sker af ond vilje. Det sker, fordi operatøren eksisterer, og alt, hvad der eksisterer, er underlagt verdens tilfældigheder.

Fraværet af en operatør er ikke underlagt de samme tilfældigheder. En retskendelse kan ikke anmode om data fra en server, der ikke eksisterer. En angriber kan ikke kompromittere en server, der ikke eksisterer. En ændring i en virksomheds politik kan ikke påvirke data, som virksomheden aldrig har haft. Nøglesætningen er enkel: Data, der ikke findes, kan ikke gå tabt.

Om det legitime argument på serversiden

Enhver, der tilbyder en professionel beskedtjeneste med en server imellem, fremfører normalt tre helt gyldige argumenter. For det første, at serveren er nødvendig for at garantere levering, når modtageren er offline. For det andet, at krypteringen af indholdet er robust, og operatøren derfor ikke kan læse det. For det tredje, at tjenesten overholder europæisk lovgivning, og at dataene er beskyttet ved lov.

Alle tre argumenter er sande. Ingen af dem ændrer sagens natur. Det er sandt, at en server tillader lagring af beskeder til senere levering; det er også sandt, at senere levering kan løses på anden vis via protokoller for direkte kommunikation mellem enheder, der er forfinet gennem årtier og fungerer i dag. Det er sandt, at kryptering af indhold under transport er robust i seriøse tjenester. Og det er sandt, at europæisk lovgivning beskytter brugere mere end i mange andre dele af verden.

Spørgsmålet er ikke, om tjenester med server imellem er lovlige, eller om de er sikre, eller om de beskytter indholdet. Det kan de være, de er lovlige, og de er normalt sikre. Spørgsmålet er, at det at have en server imellem er et arkitektonisk valg, ikke en teknisk nødvendighed. Og hvert valg har konsekvenser. En arkitektur med server imellem skaber nødvendigvis en aktør, man skal stole på. En arkitektur uden server imellem gør ikke.

Hvad loven siger, og hvad arkitekturen gør

GDPR kræver ikke en specifik arkitektonisk model. Den kræver resultater: Dataminimering, formålsbegrænsning, beskyttelse gennem design og som standard, evne til at påvise overholdelse. En tjeneste med server imellem kan opfylde alle disse krav. En tjeneste uden server imellem opfylder flere af dem ved sin konstruktion, ikke ved erklæring. Absolut minimering — ikke at indsamle noget, der ikke er strengt nødvendigt for at levere beskeden — er trivielt, når der ikke findes en server, der kan indsamle noget.

Til hverdagsbrug, der ikke er følsomt, er en arkitektur med server helt rimelig, og tillid til en seriøs operatør er en gyldig ordning. Til anden brug — det, der involverer tavshedspligt, det, der medfører etiske forpligtelser, det, der berører særligt følsomme oplysninger — er fraværet af et tillidspunkt ikke en luksus, men en strukturel fordel.

Til den professionelle læser

De spørgsmål, man bør stille sig selv i forhold til en professionel kommunikationstjeneste, som allerede er kendt fra tidligere artikler i denne serie, suppleres med blot ét arkitektonisk spørgsmål til:

1. Krypteres indholdet under transport? (Sandsynligvis ja.)
2. Genereres og gemmes der metadata om, hvem jeg taler med og hvornår? (Sandsynligvis ja.)
3. Findes der en server på vejen mellem min enhed og modtagerens?
4. Hvis der findes: Hvem driver den, i hvilken jurisdiktion, og hvad skulle der ske for at vedkommende udleverede data om mig?
5. Hvis der ikke findes: De foregående spørgsmål er irrelevante.

Forskellen mellem de to kategorier er ikke en gradsforskel, men en typeforskel. Når tiden kommer til at forklare det til en klient, en patient eller en kollega, er den mest ærlige formulering også den enkleste: I den ene er der nogen imellem; i den anden er der ikke.

Denne artikel afslutter den indledende cyklus af Cuadernos Lacre. Efter at have talt om kryptering, metadata og tavshedspligt fuldender vi det arkitektoniske billede: At kryptere indholdet og det ikke at have en server imellem er to forskellige ting. Begge kan være lovlige; kun den ene fjerner tillidspunktet.

Kilder og yderligere læsning

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Grundlæggende tekst om princippet om, at garantierne i et system skal implementeres i enderne, ikke i den mellemliggende kanal.
- Forordning (EU) 2016/679, art. 25 — databeskyttelse gennem design og som standard.
- Forordning (EU) 2016/679, art. 5.1.c — princippet 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, der minimerer indsamling gennem deres konstruktion.

← ForrigeGDPR og professionel messaging: Hvorfor de fleste overtræder reglerne uden at vide detNæste →CUADERNOS_LIST_SCHREMS_TITLE

Seneste læsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Tag denne artikel med dig, hvor du har brug for den.

↓ Markdown ↓ Almindelig tekst ↓ PDF

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 ef1f6533224b3e814d0e2d458471fb5a36f1151c7f6ea8b3d6b7de12221e1027

Cuadernos Lacre · En udgivelse fra Menzuri Gestión S.L. ·
skrevet af R.Eugenio · redigeret af holdet bag Solo2.