Analyse · 16 mei 2026

← Vorige·Volgende →

Wanneer er niemand in het midden is

Versleutelen van wat door een server gaat, beschermt de inhoud. Geen server in het midden hebben, elimineert de vraag. Het is niet hetzelfde.

Twee mensen, één gesprek

Wanneer twee mensen in een kamer gezicht tot gezicht praten, hoeft niemand te beloven dat hij niets heeft gehoord. Hij hoorde niets omdat hij er niet was. Wanneer twee mensen een papier van hand tot hand doorgeven, hoeft niemand in het midden te zweren dat hij het niet heeft gelezen. Er is niemand in het midden.

De meeste dingen in het dagelijks leven werken op deze manier. We tekenen geen geheimhoudingsverklaringen met de lucht die onze stem overbrengt, noch met het papier dat we vasthouden. De privacy van het gesprek rust niet op de belofte van een tussenpersoon, omdat er geen tussenpersoon is. Dat is een van de sterkste vormen van privé-zijn die er bestaat: niet omdat iets of iemand zich goed gedraagt, maar omdat dat iets of iemand er niet is.

Wanneer het gesprek verschuift naar een digitaal kanaal, verandert dit standaard. Het gebruikelijke model is als volgt: twee mensen maken verbinding met een server, de server ontvangt het bericht, versleutelt het of slaat het versleuteld op, en levert het af aan de ontvanger. De server staat in het midden. De server kan eerlijk zijn. Het kan geauditeerd zijn. Het kan opereren in een gunstige jurisdictie en onder een strikt privacybeleid. Dat kan allemaal waar zijn. Maar de server staat in het midden.

Het verschil tussen versleutelen en niet verzamelen (deel twee)

In een eerder artikel in deze zelfde reeks betogen we dat de inhoud versleutelen en geen metadata verzamelen niet hetzelfde zijn. Er is een verdere stap die duidelijk geformuleerd moet worden: versleutelen van wat door een server gaat en geen server hebben zijn ook niet hetzelfde.

Het eerste model — server in het midden, inhoud versleuteld — beschermt de inhoud tegen de beheerder van de server, tegen zijn onderhoudspersoneel, tegen een externe aanvaller die het systeem binnendringt. En dat is belangrijk. Maar het elimineert de server niet. De server is er nog steeds. Het verwerkt nog steeds metadata. Het is nog steeds een punt dat een gerechtelijk bevel, een juridische interventie, politieke druk of een beveiligingslek kan ontvangen. Het blijft een punt waarop vertrouwen in iemand moet worden gesteld.

Het tweede model — geen server tussen de twee uiteinden — beschermt de versleutelde inhoud niet beter: als de cryptografie robuust is, is de inhoud in beide gevallen beschermd. Wat verandert is niet de inhoud. Wat verandert is dat de vraag *«wat gebeurt er met de server?»* zijn betekenis verliest, omdat er geen server is om over te vragen.

Vertrouwen, afwezigheid, en het verschil daartussen

Vertrouwen kan goed geplaatst zijn. Eerlijke bedrijven bestaan. Strikte auditors bestaan. Gebruiksvriendelijke wetgevingen bestaan. Serieuze diensten die strikt voldoen aan al het bovenstaande bestaan. Vertrouwen, wanneer

verleend aan een beheerder die het verdient, is geen slechte regeling.

Maar vertrouwen, hoe sterk ook, blijft vertrouwen. Het is een sociale oplossing, geen technische oplossing. Een bedrijf kan van eigenaar veranderen. Een jurisdictie kan van regering veranderen. Een gerechtelijk bevel kan morgen arriveren. Een nieuwe kwetsbaarheid kan volgende maand worden ontdekt. Niets van dit alles gebeurt uit kwade trouw. Het gebeurt omdat de beheerder bestaat, en alles wat bestaat is onderhevig aan de onvoorziene omstandigheden van de wereld.

De afwezigheid van een beheerder is niet onderhevig aan diezelfde onvoorziene omstandigheden. Een gerechtelijk bevel kan geen gegevens opvragen bij een server die niet bestaat. Een aanvaller kan geen server binnendringen die niet bestaat. Een wijziging in het bedrijfsbeleid kan geen invloed hebben op gegevens die dat bedrijf nooit heeft gehad. De sleutelzin is simpel: gegevens die niet bestaan, kunnen niet verloren gaan.

Over het legitieme argument aan de serverkant

Degene die een professionele berichtendienst aanbiedt met een server in het midden, formuleert meestal drie volkomen geldige argumenten. Ten eerste, dat de server nodig is om aflevering te garanderen wanneer de ontvanger offline is. Ten tweede, dat de versleuteling van de inhoud robuust is en de beheerder deze dus niet kan lezen. Ten derde, dat de dienst voldoet aan de Europese wetgeving en dat de gegevens door de wet worden beschermd.

Alle drie de argumenten zijn waar. Geen van hen verandert de aard van de zaak. Het is waar dat een server toelaat berichten op te slaan voor vertraagde aflevering; het is ook waar dat vertraagde aflevering op een andere manier kan worden opgelost, door middel van directe communicatieprotocollen tussen apparaten die al decennia lang zijn verfijnd en vandaag de dag operationeel zijn. Het is waar dat de versleuteling van de inhoud tijdens de overdracht robuust is bij serieuze diensten. En het is waar dat de Europese wetgeving gebruikers beter beschermt dan op veel andere plaatsen.

De vraag is niet of diensten met een server in het midden legaal zijn, of ze veilig zijn, of ze de inhoud beschermen. Ze kunnen het zijn, ze zijn legaal en meestal veilig. Het punt is dat het hebben van een server in het midden een architectonische keuze is, geen technische verplichting. En elke keuze heeft gevolgen. Een architectuur met een server in het midden creëert onvermijdelijk een actor die men moet vertrouwen. Een architectuur zonder server in het midden doet dat niet.

Wat de wet zegt, en wat de architectuur doet

De AVG vereist geen specifiek architectonisch model. Het vereist resultaten: dataminimalisatie, doelbinding, gegevensbescherming door ontwerp en door standaardinstellingen, het vermogen om naleving aan te tonen. Een dienst met een server in het midden kan aan al deze eisen voldoen. Een dienst zonder server in het midden voldoet van nature aan verschillende van deze eisen, niet door declaratie. Absolute minimalisatie — niets verzamelen dat niet strikt noodzakelijk is om het bericht af te leveren — is triviaal als er geen server is die iets kan verzamelen.

Voor alledaags, niet-gevoelig gebruik is een architectuur met een server volkomen redelijk, en is vertrouwen in een serieuze beheerder een geldige regeling. Voor de andere toepassingen — degenen die een gereguleerd beroepsgeheim dragen, degenen die een deontologische verantwoordelijkheid met zich meebrengen, degenen die bijzonder gevoelige informatie raken — is de afwezigheid van een vertrouwenspunt geen luxe, het is een structureel voordeel.

Voor de professionele lezer

De vragen die men zich moet stellen bij een professionele communicatiedienst, reeds bekend uit eerdere artikelen in deze zelfde reeks, worden aangevuld met slechts één extra architectonische vraag:

1. Versleutelt het de inhoud tijdens de overdracht? (Waarschijnlijk wel.)
2. Genereert en bewaart het metadata over met wie ik spreek en wanneer? (Waarschijnlijk wel.)
3. Is er een server op de route tussen mijn apparaat en dat van de ontvanger?
4. Als deze bestaat: wie beheert deze, in welke jurisdictie, en wat zou er moeten gebeuren voordat ze gegevens over mij zouden vrijgeven?
5. Als deze niet bestaat: de voorgaande vragen zijn niet relevant.

Het verschil tussen de twee categorieën is geen gradatie, maar een type. Wanneer het tijd is om dit uit te leggen aan een cliënt, een patiënt of een collega, is de eerlijkste formulering ook de eenvoudigste: bij de ene is er iemand in het midden; bij de andere niet.

Dit artikel sluit de eerste cyclus van Cuadernos Lacre af. Na te hebben gesproken over versleuteling, metadata en beroepsgeheim, voltooien we het architectonische plaatje: de inhoud versleutelen en geen server in het midden hebben zijn verschillende dingen. Beide kunnen legaal zijn; slechts één elimineert het vertrouwenspunt.

Bronnen und verdere lectuur

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Fundamentele tekst van het principe dat de garanties van een systeem aan de uiteinden moeten worden geïmplementeerd, niet in het tussenliggende kanaal.
- Verordening (EU) 2016/679, art. 25 — gegevensbescherming door ontwerp en door standaardinstellingen.
- Verordening (EU) 2016/679, art. 5.1.c — principe van dataminimalisatie.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Hoofdstukken over architecturen die verzameling minimaliseren door ontwerp.

← VorigeAVG en zakelijke messaging: waarom de meesten onbewust in overtreding zijnVolgende →CUADERNOS_LIST_SCHREMS_TITLE

Recente artikelen

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Neem dit artikel mee naar waar u het nodig heeft.

↓ Markdown ↓ Platte tekst ↓ PDF

Het bestand wordt gedownload naar uw apparaat. Van daaruit kunt u het opslaan, importeren in Solo2 of delen waar u maar wilt. Cuadernos beslist niet voor u over de bestemming.

Lakzegel · SHA-256 9eff60f12d03cc93473b5a024987f3f5dbed16cb805c771294cffdfd040b4050

Cuadernos Lacre · Een uitgave van Menzuri Gestión S.L. ·
geschreven door R.Eugenio · geredigeerd door het team van Solo2.