Analisis · 16 Mei 2026

← Sebelumnya·Berikutnya →

Ketika tidak ada siapa-siapa di tengah

Mengenkripsi apa yang melewati server melindungi konten. Tidak memiliki server di tengah menghilangkan pertanyaan tersebut. Keduanya tidaklah sama.

Dua orang, satu percakapan

Ketika dua orang berbicara tatap muka di sebuah ruangan, tidak ada yang perlu berjanji bahwa mereka tidak mendengar apa pun. Mereka tidak mendengar karena mereka tidak ada di sana. Ketika dua orang menyerahkan selembar kertas dari satu tangan ke tangan lainnya, tidak seorang pun di tengah perlu bersumpah bahwa mereka tidak membacanya. Tidak ada siapa-siapa di tengah.

Sebagian besar hal dalam kehidupan sehari-hari bekerja dengan cara ini. Kita tidak menandatangani perjanjian kerahasiaan dengan udara yang mengirimkan suara kita, tidak juga dengan kertas yang kita pegang. Privasi percakapan tidak bergantung pada janji seorang perantara, karena tidak ada perantara. Ini adalah salah satu bentuk paling kuat yang ada untuk menjadi pribadi: bukan karena sesuatu atau seseorang berperilaku baik, tetapi karena sesuatu atau seseorang itu tidak ada.

Ketika percakapan beralih ke saluran digital, ini berubah secara default. Model yang umum adalah sebagai berikut: dua orang terhubung ke server, server menerima pesan, mengenkripsinya atau menyimpannya dalam keadaan terenkripsi, dan mengirimkannya ke penerima. Server ada di tengah. Server bisa saja jujur. Mungkin saja diaudit. Ia dapat beroperasi di yurisdiksi yang menguntungkan dan di bawah kebijakan privasi yang ketat. Semua itu mungkin benar. Namun, server ada di tengah.

Perbedaan antara mengenkripsi dan tidak mengumpulkan (bagian kedua)

Dalam artikel sebelumnya dari seri yang sama, kami berpendapat bahwa mengenkripsi konten dan tidak mengumpulkan metadata bukanlah hal yang sama. Ada satu langkah lebih jauh yang harus dirumuskan dengan jelas: mengenkripsi apa yang melewati server dan tidak memiliki server juga bukanlah hal yang sama.

Model pertama — server di tengah, konten terenkripsi — melindungi konten dari operator server, personel pemeliharaannya, dari penyerang eksternal yang menyusupi sistem. Dan itu penting. Tapi itu tidak menghilangkan server. Server masih di sana. Ia masih memproses metadata. Ia masih merupakan titik yang dapat menerima perintah pengadilan, intervensi hukum, tekanan politik, atau pelanggaran keamanan. Ini masih menjadi titik yang mengharuskan kita menaruh kepercayaan pada seseorang.

Model kedua — tidak ada server di antara dua ujung — tidak melindungi konten terenkripsi dengan lebih baik: jika kriptografinya kuat, konten dilindungi dalam kedua kasus. Yang berubah bukanlah isinya. Yang berubah adalah pertanyaan *"apa yang terjadi dengan server?"* tidak lagi relevan, karena tidak ada server untuk dipertanyakan.

Kepercayaan, ketiadaan, dan perbedaan antara keduanya

Kepercayaan mungkin ditempatkan dengan baik. Perusahaan yang jujur memang ada. Auditor yang ketat memang ada. Undang-undang yang pro-pengguna memang ada. Layanan serius yang secara ketat mematuhi semua hal di atas memang ada. Kepercayaan, ketika diberikan kepada operator yang layak menerimanya, bukanlah pengaturan yang buruk.

Tetapi kepercayaan, betapapun kuatnya, tetaplah kepercayaan. Ini adalah solusi sosial, bukan solusi teknis. Sebuah perusahaan bisa berganti pemilik. Sebuah yurisdiksi dapat mengubah pemerintahannya. Perintah pengadilan bisa tiba besok. Kerentanan baru bisa ditemukan bulan depan. Semua ini tidak terjadi karena itikad buruk. Itu terjadi karena operator ada, dan segala sesuatu yang ada tunduk pada kemungkinan yang ada di dunia.

Ketiadaan operator tidak tunduk pada kemungkinan yang sama. Perintah pengadilan tidak dapat meminta data dari server yang tidak ada. Penyerang tidak dapat menyusupi server yang tidak ada. Perubahan kebijakan perusahaan tidak dapat memengaruhi data yang tidak pernah dimiliki perusahaan tersebut. Frasa kuncinya sederhana: data yang tidak ada tidak bisa hilang.

Mengenai argumen sisi server yang sah

Siapa pun yang menawarkan layanan pesan profesional dengan server di tengah biasanya merumuskan tiga argumen yang sangat valid. Pertama, bahwa server diperlukan untuk menjamin pengiriman ketika penerima sedang offline. Kedua, bahwa enkripsi konten kuat dan karenanya operator tidak dapat membacanya. Ketiga, layanan tersebut mematuhi undang-undang Eropa dan bahwa datanya dilindungi oleh hukum.

Ketiga argumen tersebut benar. Tidak ada yang mengubah sifat masalahnya. Memang benar bahwa server memungkinkan penyimpanan pesan untuk pengiriman yang ditunda; benar juga bahwa pengiriman tertunda dapat diselesaikan dengan cara lain, melalui protokol komunikasi langsung antar perangkat yang telah disempurnakan selama puluhan tahun dan beroperasi saat ini. Memang benar bahwa enkripsi konten saat transit sangat kuat dalam layanan yang serius. Dan memang benar bahwa undang-undang Eropa melindungi pengguna lebih dari di banyak tempat lain.

Masalahnya bukan apakah layanan dengan server di tengah itu legal, atau aman, atau apakah layanan tersebut melindungi konten. Mereka mungkin begitu, mereka legal, dan mereka biasanya aman. Masalahnya adalah memiliki server di tengah adalah pilihan arsitektural, bukan pemaksaan teknis. Dan setiap pilihan memiliki konsekuensi. Arsitektur dengan server di tengah dengan sendirinya menghasilkan aktor yang harus dipercaya. Arsitektur tanpa server di tengah tidak demikian.

Apa yang dikatakan undang-undang, dan apa yang dilakukan arsitektur

GDPR tidak memerlukan model arsitektur tertentu. Ia menuntut hasil: minimalisasi data, pembatasan tujuan, perlindungan berdasarkan desain dan default, kemampuan untuk menunjukkan kepatuhan. Layanan dengan server di tengah dapat memenuhi semua persyaratan ini. Layanan tanpa server di tengah memenuhi beberapa di antaranya melalui konstruksi, bukan melalui deklarasi. Minimalisasi absolut — tidak mengumpulkan apa pun yang tidak benar-benar diperlukan untuk menyampaikan pesan — adalah sepele ketika tidak ada server yang dapat mengumpulkan apa pun.

Untuk penggunaan sehari-hari yang tidak sensitif, arsitektur dengan server sangat masuk akal, dan kepercayaan pada operator yang serius merupakan pengaturan yang sah. Untuk penggunaan lain — hal-hal yang melibatkan rahasia profesional yang diatur, hal-hal yang memerlukan tanggung jawab deontologis, hal-hal yang menyentuh informasi yang sangat sensitif — ketiadaan titik kepercayaan bukanlah sebuah kemewahan, melainkan keuntungan struktural.

Untuk pembaca profesional

Pertanyaan yang harus diajukan ketika dihadapkan pada layanan komunikasi profesional, yang sudah tidak asing lagi dari artikel sebelumnya dalam seri yang sama, dilengkapi dengan satu pertanyaan arsitektural lagi:

1. Apakah konten dienkripsi saat transit? (Mungkin ya.)
2. Apakah ia menghasilkan dan menyimpan metadata tentang dengan siapa saya berbicara dan kapan? (Mungkin ya.)
3. Apakah ada server di jalur antara perangkat saya dan perangkat penerima?
4. Jika ada: siapa yang mengoperasikannya, di yurisdiksi mana, dan apa yang harus terjadi agar mereka menyerahkan data tentang saya?
5. Jika tidak ada: pertanyaan-pertanyaan sebelumnya tidak relevan.

Perbedaan antara dua kategori ini bukanlah derajat, melainkan jenisnya. Ketika tiba waktunya untuk menjelaskannya kepada klien, pasien, atau kolega, rumusan yang paling jujur juga yang paling sederhana: di salah satu ada seseorang di tengah; di yang lain, tidak.

Artikel ini menutup siklus awal Cuadernos Lacre. Setelah berbicara tentang enkripsi, metadata, dan rahasia profesional, kita menyelesaikan gambaran arsitektur: mengenkripsi konten dan tidak memiliki server di tengah adalah hal yang berbeda. Keduanya bisa legal; hanya satu yang menghilangkan titik kepercayaan.

Sumber dan bacaan lebih lanjut

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Teks dasar dari prinsip yang menurutnya jaminan suatu sistem harus diterapkan di bagian ujung, bukan di saluran perantara.
- Peraturan (UE) 2016/679, pasal 25 — perlindungan data melalui desain dan default.
- Peraturan (UE) 2016/679, pasal 5.1.c — prinsip minimalisasi data.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Bab tentang arsitektur yang meminimalkan pengumpulan melalui desain.

← SebelumnyaGDPR dan pesan profesional: mengapa sebagian besar melanggar aturan tanpa menyadarinyaBerikutnya →CUADERNOS_LIST_SCHREMS_TITLE

Bacaan terbaru

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bawa artikel ini bersama Anda ke mana pun Anda membutuhkannya.

↓ Markdown ↓ Teks murni ↓ PDF

File akan diunduh ke perangkat Anda. Dari sana Anda dapat menyimpannya, mengimpornya ke Solo2, atau membagikannya di mana pun Anda mau. Cuadernos tidak memutuskan tujuan untuk Anda.

Segel lilin · SHA-256 d1f6285d94619a809306a203be278fd2fdf0b4da237609574392be4456e321f1

Cuadernos Lacre · Publikasi dari Menzuri Gestión S.L. ·
ditulis oleh R.Eugenio · disunting oleh tim Solo2.