Analisis · 16 Mei 2026

Apabila tiada sesiapa di tengah

Menyulitkan perkara yang melalui pelayan melindungi kandungan. Tiada pelayan di tengah menghapuskan persoalan tersebut. Ia bukan perkara yang sama.

Dua orang, satu perbualan

Apabila dua orang bercakap bersemuka di dalam sebuah bilik, tiada siapa perlu berjanji bahawa mereka tidak mendengar apa-apa. Mereka tidak mendengar kerana mereka tidak ada di sana. Apabila dua orang saling menghulurkan kertas dari satu tangan ke tangan yang lain, tiada sesiapa di tengah yang perlu bersumpah bahawa mereka tidak membacanya. Tiada sesiapa di tengah.

Kebanyakan perkara dalam kehidupan seharian berfungsi dengan cara ini. Kami tidak menandatangani perjanjian kerahsiaan dengan udara yang memancarkan suara kami, mahupun dengan kertas yang kami pegang. Privasi perbualan tidak bergantung pada janji pihak perantara, kerana tiada pihak perantara. Ini ialah salah satu bentuk kerahsiaan yang paling kukuh yang wujud: bukan kerana sesuatu atau seseorang berkelakuan baik, tetapi kerana ketiadaan sesuatu atau seseorang itu.

Apabila perbualan beralih ke saluran digital, hal ini berubah secara lalai. Model lazimnya adalah seperti berikut: dua orang menyambung ke pelayan, pelayan menerima mesej, menyulitkannya atau menyimpannya dalam keadaan disulitkan, dan menghantarnya kepada penerima. Pelayan berada di tengah. Pelayan tersebut mungkin jujur. Ia mungkin telah diaudit. Ia mungkin beroperasi dalam bidang kuasa yang menyokong dan di bawah dasar privasi yang ketat. Kesemua itu mungkin benar. Namun, pelayan tersebut berada di tengah.

Perbezaan antara penyulitan dan ketiadaan pengumpulan (bahagian kedua)

Dalam artikel sebelum ini dalam siri yang sama ini, kami berpendapat bahawa penyulitan kandungan dan bukan pengumpulan metadata adalah perkara yang berbeza. Terdapat langkah lebih jauh yang perlu dirumuskan dengan jelas: menyulitkan apa yang melalui pelayan dan tidak mempunyai pelayan juga bukanlah perkara yang sama.

Model pertama — pelayan di tengah, kandungan disulitkan — melindungi kandungan daripada pengendali pelayan, petugas penyelenggaraannya, daripada penyerang luar yang menjejaskan sistem. Dan itu adalah penting. Tetapi ia tidak menghapuskan pelayan. Pelayan tersebut masih ada. Ia masih memproses metadata. Ia kekal sebagai sasaran yang boleh menerima arahan mahkamah, campur tangan undang-undang, tekanan politik, atau pelanggaran keselamatan. Ia tetap menjadi titik yang memerlukan anda meletakkan kepercayaan kepada seseorang.

Model kedua — tiada pelayan antara dua hujung — tidak semestinya lebih baik dalam melindungi kandungan yang disulitkan: jika kriptografi kukuh, kandungannya terpelihara dalam kedua-dua keadaan. Apa yang berubah bukanlah kandungan. Apa yang berubah ialah soalan *«apa yang berlaku dengan pelayan?»* menjadi tidak relevan, kerana tiada pelayan untuk dipersoalkan.

Kepercayaan, ketiadaan, dan perbezaan antara keduanya

Kepercayaan mungkin diletakkan pada tempat yang betul. Syarikat yang jujur memang wujud. Juruaudit yang teliti memang wujud. Undang-undang yang memihak kepada pengguna memang wujud. Perkhidmatan serius yang teliti mematuhi semua perkara di atas memang wujud. Kepercayaan, apabila diberikan kepada pengendali yang layak, bukanlah suatu pengaturan yang buruk.

Tetapi kepercayaan, walau sekukuh mana pun, tetap merupakan kepercayaan. Ia adalah penyelesaian sosial, bukan penyelesaian teknikal. Syarikat boleh bertukar tangan. Bidang kuasa boleh bertukar kerajaan. Arahan mahkamah mungkin tiba pada esok hari. Kelemahan baharu mungkin ditemui pada bulan hadapan. Semua ini tidak berlaku atas niat buruk. Ia berlaku kerana pengendali itu wujud, dan segala-galanya yang wujud tertakluk pada kemungkinan yang berlaku di dunia.

Ketiadaan pengendali tidak tertakluk kepada kemungkinan yang sama. Perintah mahkamah tidak boleh meminta data daripada pelayan yang tidak wujud. Penyerang tidak boleh menjejaskan pelayan yang tidak wujud. Perubahan dalam polisi syarikat tidak boleh menjejaskan data yang syarikat itu tidak pernah miliki. Frasa kuncinya adalah mudah: data yang tidak wujud tidak boleh hilang.

Mengenai hujah yang sah di pihak pelayan

Sesiapa yang menawarkan perkhidmatan pemesejan profesional dengan pelayan di tengah biasanya mengemukakan tiga hujah yang sah sepenuhnya. Pertama, pelayan diperlukan untuk menjamin penghantaran apabila penerima berada di luar talian. Kedua, penyulitan kandungan adalah mantap dan oleh itu pengendali tidak boleh membacanya. Ketiga, perkhidmatan tersebut mematuhi perundangan Eropah dan data dilindungi oleh undang-undang.

Ketiga-tiga hujah itu adalah benar. Tiada satupun yang mengubah sifat perkara itu. Memang benar bahawa pelayan membenarkan penyimpanan mesej untuk penghantaran tertunda; juga benar bahawa penghantaran tertunda boleh diselesaikan dengan cara lain, melalui protokol komunikasi langsung antara peranti yang telah diperhalusi selama berdekad-dekad dan beroperasi hari ini. Memang benar penyulitan kandungan dalam transit adalah mantap dalam perkhidmatan yang serius. Dan memang benar perundangan Eropah melindungi penggunanya melebihi banyak tempat lain.

Persoalannya bukan sama ada perkhidmatan yang menggunakan pelayan di tengah itu sah, sama ada ianya selamat, atau sama ada ia melindungi kandungan. Ia mungkin sedemikian, ia adalah sah, dan ia lazimnya selamat. Isunya ialah mempunyai pelayan di tengah-tengah ialah suatu pilihan seni bina, bukannya tuntutan teknikal. Dan setiap pilihan ada akibatnya. Seni bina dengan pelayan di tengah semestinya mewujudkan satu pelakon yang mesti diberi kepercayaan. Sebaliknya, seni bina tanpa pelayan di tengah tidak memerlukan hal tersebut.

Apa yang dikatakan oleh undang-undang, dan apa yang dilakukan oleh seni bina

GDPR tidak memerlukan model seni bina yang khusus. Ia menuntut hasil: meminimumkan data, had tujuan, perlindungan reka bentuk secara lalai, serta keupayaan membuktikan pematuhan. Perkhidmatan dengan pelayan di tengah boleh memenuhi segala keperluan ini. Perkhidmatan tanpa pelayan di tengah memenuhi kebanyakannya secara semula jadi menurut struktur binaan, bukan sekadar deklarasi. Peminimuman mutlak — tidak mengumpul apa-apa yang tidak benar-benar perlu untuk menghantar mesej — adalah mudah apabila tiada pelayan yang dapat mengumpulkan apa-apa.

Untuk penggunaan harian yang tidak sensitif, penggunaan seni bina pelayan ialah wajar, dan meletakkan kepercayaan kepada pengendali yang serius merupakan tindakan yang munasabah. Untuk kegunaan lain — yang melibatkan kerahsiaan profesional terkawal, yang membawa tanggungjawab deontologi, yang menyentuh maklumat yang sangat sensitif — ketiadaan titik kepercayaan bukanlah satu kemewahan, ia adalah kelebihan struktur.

Bagi pembaca profesional

Soalan-soalan yang perlu ditanya mengenai perkhidmatan komunikasi profesional, yang telah pun diketahui dalam artikel sebelumnya dalam siri ini, dilengkapkan dengan satu lagi soalan seni bina:

1. Adakah ia menyulitkan kandungan dalam transit? (Mungkin ya.)
2. Adakah ia menjana dan menyimpan metadata mengenai dengan siapa dan bila saya bercakap? (Mungkin ya.)
3. Adakah terdapat pelayan di laluan antara peranti saya dengan penerima?
4. Jika ada: siapakah yang mengendalikannya, di bawah bidang kuasa manakah ia, dan apakah yang perlu berlaku sebelum ia menyerahkan data saya?
5. Jika tidak ada: soalan di atas adalah tidak relevan.

Perbezaan antara kedua-dua kategori ini bukan daripada tahap, tetapi jenis. Apabila tiba masanya untuk menerangkan hal tersebut kepada pelanggan, pesakit atau rakan sekerja, perumusan yang paling jujur juga adalah yang paling mudah: salah satunya mempunyai seseorang di tengah; manakala satu lagi, tiada.

Artikel ini menutup kitaran awal Cuadernos Lacre. Selepas bercakap tentang penyulitan, metadata dan rahsia profesional, kami melengkapkan gambaran seni bina: menyulitkan kandungan dan tidak mempunyai pelayan di tengah adalah perkara yang berbeza. Kedua-duanya boleh jadi sah di sisi undang-undang; hanya satu yang menghapuskan titik kepercayaan.

Sumber dan bacaan lanjut

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Teks asas untuk prinsip di mana jaminan sistem mesti dilaksanakan pada hujung sambungan, bukan dalam saluran perantara.
- Peraturan (EU) 2016/679, fasal 25 — perlindungan data melalui reka bentuk dan secara lalai.
- Peraturan (EU) 2016/679, fasal 5.1.c — prinsip meminimumkan data.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Bab tentang seni bina yang meminimumkan pengumpulan mengikut reka bentuk binaan.

← SebelumnyaGDPR dan pemesejan profesional: mengapa kebanyakan melanggar peraturan tanpa menyedarinyaSeterusnya →CUADERNOS_LIST_SCHREMS_TITLE

Bacaan terkini

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bawa artikel ini bersama anda ke mana sahaja anda memerlukannya.

↓ Markdown ↓ Teks biasa ↓ PDF

Fail akan dimuat turun ke peranti anda. Dari sana anda boleh menyimpannya, mengimportnya ke Solo2, atau berkongsinya di mana sahaja anda mahu. Cuadernos tidak memutuskan destinasi untuk anda.

Mohor lilin · SHA-256 971766bcb89b5680d0d5dea630cb35fb4851e4f2841a35184600f2ca6dc1609c

Cuadernos Lacre · Penerbitan daripada Menzuri Gestión S.L. ·
ditulis oleh R.Eugenio · disunting oleh pasukan Solo2.