Enkripsi tidak berarti privasi: apa yang dikatakan metadata tentang Anda

Konten terenkripsi dan metadata yang terlihat adalah dua hal yang berbeda. Ketika sebuah layanan berbicara tentang "enkripsi end-to-end", itu hanya menceritakan setengah dari ceritanya.

Gembok yang tidak melindungi segalanya

Sebagian besar layanan pesan saat ini mengiklankan enkripsi end-to-end. Dan itu benar: isi pesan dikirimkan dalam keadaan terenkripsi, sehingga tidak ada seorang pun di tengah jalan – bahkan penyedia layanan sekalipun – yang dapat membaca teks tersebut saat sedang dikirim. Sampai di sini, pernyataannya akurat.

Masalahnya adalah konten hanyalah sebagian dari cerita. Meskipun tidak ada yang bisa membaca apa yang Anda katakan, layanan tersebut mengetahui hal-hal lain dengan presisi yang sangat tinggi: dengan siapa Anda berbicara, pada jam berapa, seberapa sering, dari lokasi mana kira-kira, di perangkat apa, berapa banyak pesan yang Anda kirim dan berapa banyak yang Anda terima, berapa banyak file yang Anda bagikan. Semua ini disebut metadata. Dan metadata, dalam banyak kasus, mengatakan hampir sebanyak pesan itu sendiri.

Apa yang diungkapkan metadata

Seseorang tidak perlu membaca pesan untuk mengetahui banyak hal. Jika seseorang menelepon atau menulis pesan kepada seorang ahli onkologi setiap Selasa pagi jam sembilan selama enam bulan, tidak perlu mendengar percakapan tersebut untuk menduga apa yang sedang terjadi. Jika dua orang bertukar seratus pesan sehari dan tiba-tiba berhenti melakukannya, Anda tidak perlu membaca satu pun untuk memahami apa yang telah terjadi. Jika seorang konsultan pajak menerima dua puluh pesan berturut-turut dari klien yang sama pada malam sebelum penutupan kuartalan, polanya berbicara sendiri.

Metadata mengungkapkan pola perilaku: siapa yang berhubungan dengan siapa, apa jadwal setiap orang, kapan mereka bangun, kapan mereka tidur, kapan mereka bepergian, klien mana yang paling aktif, hubungan profesional mana yang paling intens. Server yang mengumpulkan metadata dapat membangun profil mendalam tentang kehidupan pribadi dan profesional pengguna mana pun tanpa pernah membaca satu kata pun dari apa yang dia tulis.

Ada contoh historis yang menggambarkan hal ini dengan keras. Mantan direktur NSA, Michael Hayden, merumuskannya secara blak-blakan pada tahun 2014: *"We kill people based on metadata"*. Pernyataan tersebut merujuk pada operasi militer AS terhadap sasaran yang diidentifikasi secara eksklusif berdasarkan pola komunikasi mereka. Tidak ada satu pun pesan yang dibaca. Hanya grafik kontak dan jadwal.

Bahwa suatu layanan mengumpulkan metadata tidak selalu berarti ia akan menggunakannya untuk melawan penggunanya. Ini berarti ia memiliki kapasitas untuk melakukannya, dan bahwa pihak ketiga dengan akses ke data tersebut – melalui perintah pengadilan, melalui pelanggaran keamanan, atau melalui penjualan kepada pihak ketiga jika ketentuan layanan mengizinkannya – juga memilikinya.

Akses ke buku kontak

Vektor lain yang hampir tidak diperhatikan: daftar kontak. Sebagian besar layanan pesan meminta akses ke buku kontak telepon saat mendaftar. Mereka mengunggah semua nomor ke server mereka untuk menunjukkan siapa lagi yang menggunakan layanan tersebut. Sejak saat itu, perusahaan memiliki peta lengkap hubungan pengguna, bahkan jika dia belum pernah menulis satu pesan pun kepada siapa pun.

Bagi seorang profesional yang tunduk pada rahasia profesi – pengacara, dokter, psikolog, konsultan – buku kontak tersebut berisi klien. Jika buku kontak telah diunggah ke server pihak ketiga, nama-nama klien berada dalam infrastruktur yang yurisdiksi dan kebijakannya tidak dikendalikan oleh profesional tersebut. Rahasia profesi tidak rusak pada hari seseorang membocorkan percakapan: rahasia itu sudah rusak jauh sebelumnya, pada saat persetujuan pengunggahan.

Perbedaan antara mengenkripsi dan tidak mengumpulkan

Mengenkripsi berarti melindungi konten. Menjadi pribadi berarti tidak mengumpulkan apa yang tidak diperlukan. Ini adalah hal yang berbeda, dan perbedaannya sangat krusial secara operasional. Sebuah layanan dapat mengenkripsi semua pesan dengan sempurna dan pada saat yang sama mengetahui hampir segalanya tentang penggunanya melalui metadata. Keduanya sangat kompatibel. Faktanya, ini adalah model bisnis yang dominan di sektor ini.

Pertanyaan yang tepat untuk mengevaluasi privasi sebenarnya dari sebuah layanan bukanlah *"apakah ia mengenkripsi konten?"*. Pertanyaan itu telah terjawab selama bertahun-tahun. Pertanyaan yang tepat adalah: *"metadata apa yang dihasilkannya dan di mana ia disimpan?"*. Dan yang terpenting: *"metadata apa yang tidak perlu dihasilkannya?"*.

Arsitektur yang meminimalkan metadata melalui desain – bukan melalui janji, bukan melalui kebijakan internal – secara struktural lebih pribadi daripada arsitektur yang mengumpulkan dan mengenkripsinya. Karena data yang tidak ada tidak dapat dibocorkan, tidak dapat dijual, tidak dapat diserahkan ke perintah pengadilan atau hilang dalam pelanggaran keamanan.

Untuk pembaca profesional

Jika aktivitas profesional Anda melibatkan rahasia, kerahasiaan, atau sekadar menghormati informasi pihak ketiga, ada baiknya mengajukan pertanyaan dalam urutan ini:

1. Apakah aplikasi yang saya gunakan untuk berkomunikasi mengenkripsi konten? (Mungkin ya.)
2. Apakah ia mengenkripsi metadata? (Mungkin tidak.)
3. Apakah ia menghasilkan metadata yang *tidak diperlukannya* untuk beroperasi? (Hampir pasti ya.)
4. Di mana metadata itu disimpan dan di bawah yurisdiksi mana? (Kemungkinan besar di luar Wilayah Ekonomi Eropa.)
5. Apakah klien atau pasien saya tahu bahwa datanya ada di sana?

Pertanyaan terakhir adalah yang tidak nyaman. Karena jawaban jujurnya dalam banyak kasus adalah: tidak.

Artikel ini adalah yang pertama dalam seri tentang cara kerja sebenarnya dari alat komunikasi profesional. Edisi berikutnya akan membahas kepatuhan GDPR dalam pesan dan konsep rahasia profesi di era digital.

Sumber dan bacaan lebih lanjut

- Hayden, M. – Pernyataan di Universitas Johns Hopkins, 2014 ("We kill people based on metadata"). Transkrip publik tersedia.
- GDPR (Peraturan Uni Eropa 2016/679), Pasal 4 dan 5 – definisi data pribadi dan prinsip-prinsip pemrosesan (metadata adalah data pribadi).
- EDPS dan EDPB – pendapat tentang pemrosesan data lalu lintas dan metadata dalam komunikasi elektronik (petunjuk ePrivacy).

← SebelumnyaSejarah singkat segel lilinBerikutnya →Rahasia profesi di era digital

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 bfaa9e51139b7fc734dc745c9828ad14c34001fc299b0dd843bdbce9d941a82e

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