Аналіз · 16 травня 2026 р.

← Попередній·Наступний →

Шифрування не означає конфіденційність: що метадані говорять про вас

Зашифрований вміст і видимі метадані — це дві різні речі. Коли сервіс говорить про «наскрізне шифрування», він розповідає лише половину історії.

Замок, який не захищає все

Велика частина сучасних месенджерів рекламує наскрізне шифрування. І це правда: вміст повідомлень передається зашифрованим, так що ніхто в дорозі — навіть постачальник послуг — не може прочитати текст під час передачі. До цього моменту твердження є точним.

Проблема в тому, що вміст — це лише частина історії. Навіть якщо ніхто не може прочитати те, що ви кажете, сервіс знає інші речі з дуже високою точністю: з ким ви розмовляєте, о котрій годині, як часто, з якого приблизного місця розташування, на якому пристрої, скільки повідомлень ви надсилаєте і скільки отримуєте, скільки файлів ви поширюєте. Все це називається метаданими (metadata). І метадані в багатьох випадках говорять майже стільки ж, скільки саме повідомлення.

Що розкривають метадані

Не потрібно читати повідомлення, щоб знати багато речей. Якщо людина телефонує або пише онкологу щовівторка вранці о дев'ятій годині протягом шести місяців, не обов'язково чути розмову, щоб здогадатися, що відбувається. Якщо двоє людей обмінюються сотнею повідомлень на день і раптом припиняють це робити, не потрібно читати жодного, щоб зрозуміти, що сталося. Якщо податковий консультант отримує двадцять повідомлень поспіль від одного і того ж клієнта в ніч перед квартальним закриттям, модель говорить сама за себе.

Метадані розкривають поведінкові моделі: хто з ким у стосунках, які графіки у кожної людини, коли вони не сплять, коли сплять, коли подорожують, які клієнти найбільш активні, які професійні відносини найбільш інтенсивні. Сервер, який збирає метадані, може побудувати детальний профіль особистого та професійного життя будь-якого користувача, ніколи не прочитавши жодного слова з того, що він пише.

Є історичний приклад, який ілюструє це жорстко. Колишній директор NSA Майкл Хайден сформулював це прямо у 2014 році: *«We kill people based on metadata»*. Заява стосувалася військових операцій США проти цілей, ідентифікованих виключно на основі їхніх моделей комунікації. Жодного прочитаного повідомлення. Тільки граф контактів і графіки.

Те, що сервіс збирає метадані, не обов'язково означає, що він використовуватиме їх проти своїх користувачів. Це означає, что він має таку можливість, і що третя сторона з доступом до цих даних — за рішенням суду, через порушення безпеки або через продаж третім особам, якщо умови надання послуг це дозволяють — також має її.

Доступ до адресної книги

Ще один вектор, який проходить майже непоміченим: список контактів. Велика частина месенджерів просить доступ до адресної книги телефону під час реєстрації. Вони завантажують усі номери на свій сервер, щоб показати, хто ще користується сервісом. З цього моменту компанія має повну карту стосунків користувача, навіть якщо він ніколи нікому не написав жодного повідомлення.

Для професіонала, на якого поширюється професійна таємниця — адвоката, лікаря, психолога, консультанта — ця адресна книга містить клієнтів. Якщо адресна книга була завантажена на сервер третьої сторони, імена клієнтів знаходяться в інфраструктурі, юрисдикцію та політику якої професіонал не контролює. Професійна таємниця не порушується в той день, коли хтось зливає розмову: вона була порушена набагато раніше, в момент згоди на завантаження.

Різниця між шифруванням та незбиранням

Шифрувати — означає захищати вміст. Бути приватним — означає не збирати те, що не потрібно. Це різні речі, і різниця є операційно вирішальною. Сервіс може ідеально шифрувати всі повідомлення і водночас знати майже все про своїх користувачів через метадані. Обидва варіанти цілком сумісні. Насправді це домінуюча бізнес-модель у секторі.

Правильне питання для оцінки справжньої конфіденційності сервісу — не *«чи шифрує він вміст?»*. На це питання відповідь відома вже багато років. Правильне питання таке: *«які метадані він генерує і де вони зберігаються?»*. І, перш за все: *«які метадані йому не потрібно генерувати?»*.

Архітектура, яка мінімізує метадані за дизайном (privacy by design) — не за обіцянкою, не за внутрішньою політикою — є структурно більш приватною, ніж архітектура, яка їх збирає та шифрує. Тому що дані, яких не існує, не можуть бути злиті, продані, передані за рішенням суду або втрачені під час зламу.

Для професійного читача

Якщо ваша професійна діяльність пов'язана з таємницею, конфіденційністю або просто повагою до інформації третіх осіб, варто поставити питання в такому порядку:

1. Чи шифрує додаток, який я використовую для спілкування, вміст? (Ймовірно, так.)
2. Чи шифрує він метадані? (Ймовірно, ні.)
3. Чи генерує він метадані, які йому *не потрібні* для роботи? (Майже напевно, так.)
4. Де зберігаються ці метадані та під якою юрисдикцією? (Ймовірно, за межами Європейського економічного простору.)
5. Чи знає мій клієнт або пацієнт, що його дані там?

Останнє питання — незручне. Тому що чесна відповідь у більшості випадків: ні.

Ця стаття є першою в серії про реальну роботу професійних інструментів комунікації. Наступні випуски будуть присвячені дотриманню GDPR у месенджерах та концепції професійної таємниці в цифрову епоху.

Джерела та додаткова література

- Хайден, М. — Заява в Університеті Джонса Гопкінса, 2014 р. («We kill people based on metadata»). Доступні публічні стенограми.

- GDPR (Регламент ЄС 2016/679), ст. 4 та 5 — визначення персональних даних та принципи обробки (метадані є персональними даними).
- Європейський інспектор з захисту даних та EDPB — висновки щодо обробки даних трафіку та метаданих в електронних комунікаціях (директива ePrivacy).

← ПопереднійКоротка історія сургучної печаткиНаступний →Професійна таємниця в цифрову епоху

Останні матеріали

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 8c1abc25aebb84c28521367032e9e080fac11a4e84fe5467a3c7448fd84604f1

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.