Анализ · 16 май 2026 г.

← Предишна·Следваща →

Криптирането не е поверителност: какво казват метаданните за вас

Криптираното съдържание и видимите метаданни са две различни неща. Когато една услуга говори за „криптиране от край до край“, тя разказва само половината история.

Катинарът, който не защитава всичко

Голяма част от днешните услуги за съобщения рекламират криптиране от край до край. И това е вярно: съдържанието на съобщенията пътува криптирано, така че никой по пътя – дори доставчикът на услугата – не може да прочете текста, докато се предава. Дотук твърдението е точно.

Проблемът е, че съдържанието е само част от историята. Въпреки че никой не може да прочете какво казвате, услугата знае други неща с много висока точност: с кого говорите, по кое време, колко често, от какво приблизително местоположение, на какво устройство, колко съобщения изпращате и колко получавате, колко файла споделяте. Всичко това се нарича метаданни. А метаданните в много случаи казват почти толкова, колкото и самото съобщение.

Какво разкриват метаданните

Не е необходимо да се чете съобщение, за да се знаят много неща. Ако човек се обажда или пише на онколог всеки вторник сутрин в девет часа в продължение на шест месеца, не е необходимо да се слуша разговорът, за да се предположи какво става. Ако двама души обменят сто съобщения на ден и изведнъж спрат, не е необходимо да четете нито едно, за да разберете какво се е случило. Ако данъчен консултант получи двадесет съобщения подред от един и същ клиент в нощта преди тримесечно приключване, моделът говори сам за себе си.

Метаданните разкриват поведенчески модели: кой с кого е в отношения, какви графици има всеки човек, кога е буден, кога спи, кога пътува, кои клиенти са най-активни, кои професионални отношения са най-интензивни. Сървър, който събира метаданни, може да изгради подробен профил на личния и професионалния живот на всеки потребител, без някога да е прочел нито една дума от това, което той пише.

Има исторически пример, който илюстрира това твърдо. Бившият директор на NSA Майкъл Хейдън го формулира направо през 2014 г.: *„We kill people based on metadata“*. Твърдението се отнасяше за американски военни операции срещу цели, идентифицирани изключително въз основа на техните комуникационни модели. Нито едно прочетено съобщение. Само графика на контактите и графиците.

Това, че една услуга събира метаданни, не означава непременно, че ще ги използва срещу потребителите си. Означава, че има способността да го направи и че трета страна с достъп до тези данни – чрез съдебно разпореждане, чрез пробив в сигурността или чрез продажба на трети страни, ако условията на услугата го позволяват – също я има.

Достъпът до адресната книга

Друг вектор, който преминава почти незабелязано: списъкът с контакти. Голяма част от услугите за съобщения искат достъп до адресната книга на телефона при регистрация. Те качват всички номера на своя сървър, за да покажат кой друг използва услугата. От този момент компанията има пълна карта на отношенията на потребителя, дори ако той никога не е писал нито едно съобщение на никого.

За професионалист, обвързан с професионална тайна – адвокат, лекар, психолог, консултант – тази адресна книга съдържа клиенти. Ако адресната книга е качена на сървър на трета страна, имената на клиентите се намират в инфраструктура, чиято юрисдикция и политики професионалистът не контролира. Професионалната тайна не се нарушава в деня, в който някой изтече разговор: тя е била нарушена много по-рано, в момента на съгласието за качване.

Разликата между криптиране и несъбиране

Криптирането е защита на съдържанието. Поверителността е несъбиране на това, което не е необходимо. Това са различни неща и разликата е оперативно решаваща. Една услуга може перфектно да криптира всички съобщения и същевременно да знае почти всичко за потребителите си чрез метаданни. И двете неща са напълно съвместими. Всъщност това е доминиращият бизнес модел в сектора.

Правилният въпрос за оценка на действителната поверителност на една услуга не е *„криптира ли съдържанието?“*. На този въпрос е отговорено от години. Правилният въпрос е: *„какви метаданни генерира и къде се съхраняват?“*. И преди всичко: *„какви метаданни не е необходимо да генерира?“*.

Архитектура, която минимизира метаданните чрез дизайн – не чрез обещание, не чрез вътрешна политика – е структурно по-поверителна от архитектура, която ги събира и криптира. Тъй като данни, които не съществуват, не могат да бъдат изтекли, нито продадени, нито предадени на съдебно разпореждане или изгубени при пробив в сигурността.

За професионалния читател

Ако вашата професионална дейност включва тайна, поверителност или просто уважение към информацията на трети страни, си струва да зададете въпросите в този ред:

1. Криптира ли приложението, което използвам за комуникация, съдържанието? (Вероятно да.)
2. Криптира ли метаданните? (Вероятно не.)
3. Генерира ли метаданни, от които *не се нуждае*, за да функционира? (Почти сигурно да.)
4. Къде се съхраняват тези метаданни и под каква юрисдикция? (Вероятно извън Европейското икономическо пространство.)
5. Знае ли моят клиент или пациент, че данните му са там?

Последният въпрос е неудобният. Защото честният отговор в повечето случаи е: не.

Тази статия е първата от поредица за реалното функциониране на професионалните инструменти за комуникация. Следващите броеве ще разгледат спазването на GDPR при съобщенията и концепцията за професионална тайна в цифровата ера.

Източници и допълнително четиво

- Hayden, M. – Декларация в университета Джонс Хопкинс, 2014 г. („We kill people based on metadata“). Налични публични транскрипции.

- GDPR (Регламент на ЕС 2016/679), чл. 4 и 5 – определение за лични данни и принципи на обработване (метаданните са лични данни).
- ЕНОЗД и EDPB – становища относно обработването на данни за трафика и метаданни в електронните съобщения (Директива за правото на неприкосновеност на личния живот в електронните съобщения).

← ПредишнаКратка история на печатната смолаСледваща →Професионалната тайна в цифровата ера

Скорошни четива

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Вземете тази статия със себе си навсякъде, където ви е необходима.

↓ Markdown ↓ Обикновен текст ↓ PDF

Файлът ще бъде изтеглен на вашето устройство. Оттам можете да го запазите, импортирате в Solo2 или споделите където пожелаете. Cuadernos не решава дестинацията вместо вас.

Восъчен печат · SHA-256 167485abe4c300c78622f12b5361ec19cf9a3b6b483fa2973c9412a3504e2537

Cuadernos Lacre · Публикация на Menzuri Gestión S.L. ·
написана от R.Eugenio · редактирана от екипа на Solo2.