Анализ · 16 май 2026 г.

← Предишна·Следваща →

Когато няма никой по средата

Шифроването на това, което преминава през сървър, защитава съдържанието. Липсата на сървър по средата премахва въпроса. Те не са едно и също.

Двама души, един разговор

Когато двама души разговарят лице в лице в една стая, никой не трябва да обещава, че не е чул нищо. Той не е чул, защото не е бил там. Когато двама души си подават хартия от ръка на ръка, никой по средата не трябва да се кълне, че не я е чел. По средата няма никой.

Повечето неща в ежедневието функционират по този начин. Не подписваме споразумения за поверителност с въздуха, който предава гласа ни, нито с хартията, която държим. Поверителността на разговора не се основава на обещанието на посредник, защото няма посредник. Това е един от най-силните начини за поверителност: не защото нещо или някой се държи добре, а защото нещо или някой изобщо не съществува.

Когато разговорът се премести в цифров канал, това се променя по подразбиране. Обичайният модел е следният: двама души се свързват със сървър, сървърът получава съобщението, шифрова го или го съхранява шифровано и го доставя на получателя. Сървърът е по средата. Сървърът може да бъде честен. Може да бъде одитиран. Може да работи в благоприятна юрисдикция и под строга политика за поверителност. Всичко това може да е вярно. Но сървърът е по средата.

Разликата между шифроване и несъбиране (втора част)

В предишна статия от същата поредица твърдим, че шифроването на съдържанието и несъбирането на метаданни не са едно и също нещо. Има още една стъпка напред, която е добре да формулираме ясно: шифроването на това, което преминава през сървър, и липсата на сървър също не са едно и също нещо.

Първият модел — сървър по средата, шифровано съдържание — защитава съдържанието от оператора на сървъра, от неговия поддържащ персонал, от външен нападател, който компрометира системата. И това е важно. Но то не премахва сървъра. Сървърът все още е там. Той все още обработва метаданни. Той все още е точка, която може да получи съдебно разпореждане, законна намеса, политически натиск или пробив в сигурността. Той все още е точка, която изисква гласуване на доверие на някого.

Вторият модел — липсата на сървър между двете крайни точки — не защитава по-добре шифрованото съдържание: ако криптографията е солидна, съдържанието е защитено и в двата случая. Това, което се променя, не е съдържанието. Това, което се променя, е че въпросът *„какво става със сървъра?“* губи своя предмет, защото не съществува сървър, за който да се пита.

Доверие, отсъствие и разликата между тях

Доверието може да бъде добре гласувано. Съществуват честни компании. Съществуват строги одитори. Съществуват законодателства, благоприятни за потребителя. Съществуват сериозни услуги, които спазват стриктно всичко изброено по-горе. Доверието, когато се предоставя на оператор, който го заслужава, не е лоша уговорка.

Но доверието, колкото и да е солидно, си остава доверие. Това е социално решение, а не техническо решение. Една компания може да смени собственика си. Една юрисдикция може да смени правителството си. Едно съдебно разпореждане може да пристигне утре. Една нова уязвимост може да бъде открита следващия месец. Нищо от това не се случва поради лоша воля. Случва се, защото операторът съществува, а всичко съществуващо е обект на случайностите в света.

Отсъствието на оператор не е обект на същите тези случайности. Едно съдебно разпореждане не може да изисква данни от сървър, който не съществува. Един нападател не може да компрометира сървър, който не съществува. Промяна в политиката на една компания не може да засегне данни, които тази компания никога не е имала. Ключовата фраза е проста: данните, които не съществуват, не могат да бъдат загубени.

Относно легитимния аргумент от страна на сървъра

Всеки, който предлага професионална услуга за съобщения със сървър по средата, обикновено изтъква три напълно валидни аргумента. Първо, че сървърът е необходим, за да гарантира доставката, когато получателят е офлайн. Второ, че шифроването на съдържанието е стабилно и следователно операторът не може да го прочете. Трето, че услугата спазва европейското законодателство и че данните са защитени от закона.

И трите аргумента са верни. Никой от тях не променя същността на въпроса. Вярно е, че един сървър позволява съхраняване на съобщения за забавена доставка; също така е вярно, че забавената доставка може да бъде решена по друг начин чрез протоколи за директна комуникация между устройства, прецизирани от десетилетия и действащи днес. Вярно е, че шифроването на съдържанието при транзит е стабилно в сериозните услуги. И е вярно, че европейското законодателство защитава потребителите повече от това на много други места.

Въпросът не е дали услугите със сървър по средата са законни, нито дали са сигурни, нито дали защитават съдържанието. Те могат да бъдат такива, те са законни и обикновено са сигурни. Въпросът е, че наличието на сървър по средата е архитектурен избор, а не техническа наложеност. И всеки избор има последствия. Архитектура със сървър по средата неизбежно създава участник, на когото трябва да се вярва. Архитектура без сървър по средата — не.

Това, което законът казва, и това, което архитектурата прави

GDPR не изисква конкретен архитектурен модел. Изисква резултати: минимизиране на данните, ограничена цел, защита по дизайн и по подразбиране, способност за доказване на съответствието. Една услуга със сървър по средата може да отговаря на всички тези изисквания. Една услуга без сървър по средата отговаря на няколко от тях чрез конструкцията си, а не чрез декларация. Абсолютното минимизиране — несъбирането на нищо, което не е строго необходимо за доставяне на съобщението — е тривиално, когато не съществува сървър, който да събере нещо.

За ежедневни нечувствителни нужди архитектурата със сървър е напълно разумна и доверието в сериозен оператор е валидна уговорка. За другите нужди — тези, които включват регламентирана професионална тайна, тези, които носят етична отговорност, тези, които засягат особено чувствителна информация — липсата на точка на доверие не е лукс, а структурно предимство.

За професионалния читател

Въпросите, които е добре да си зададем пред една професионална комуникационна услуга, вече познати от предишни статии в тази серия, се допълват само с още един архитектурен въпрос:

1. Шифрова ли съдържанието при транзит? (Вероятно да.)
2. Генерира ли и съхранява ли метаданни за това с кого говоря и кога? (Вероятно да.)
3. Съществува ли сървър по пътя между моето устройство и това на получателя?
4. Ако съществува: кой го управлява, в коя юрисдикция и какво трябва да се случи, за да предаде данни за мен?
5. Ако не съществува: предишните въпроси нямат обект.

Разликата между двете категории не е в степента, а във вида. Когато дойде моментът да го обясните на клиент, пациент или колега, най-честната формулировка е и най-простата: в единия случай има някой по средата, в другия — не.

Тази статия затваря първоначалния цикъл на Cuadernos Lacre. След като говорихме за шифроването, метаданните и професионалната тайна, допълваме архитектурната картина: шифроването на съдържанието и липсата на сървър по средата са различни неща. И двете могат да бъдат законни; само едната премахва точката на доверие.

Източници и допълнително четиво

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Основополагащ текст на принципа, според който гаранциите на една система трябва да се прилагат в краищата, а не в междинния канал.
- Регламент (ЕС) 2016/679, чл. 25 — защита на данните на етапа на проектирането и по подразбиране.
- Регламент (ЕС) 2016/679, чл. 5.1.в — принцип на минимизиране на данните.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Глави за архитектури, които минимизират събирането чрез конструкцията си.

← ПредишнаGDPR и професионалните съобщения: защо повечето хора нарушават правилата, без да го знаятСледваща →CUADERNOS_LIST_SCHREMS_TITLE

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 53ad34bbcca4419093561575e8970ceb985813e90ec7430858f672b89aba650c

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

необходим за предпочитанието ви за светла/тъмна тема. Без тракери, без профилиране, без споделяне на данни. Ако искате да ни последвате: RSS.