Gdy nie ma nikogo pośrodku

Szyfrowanie tego, co przechodzi przez serwer, chroni treść. Brak serwera pośrodku eliminuje pytanie. To nie jest to samo.

Dwie osoby, jedna rozmowa

Gdy dwie osoby rozmawiają twarzą w twarz w pokoju, nikt nie musi obiecywać, że nic nie słyszał. Nie słyszał, bo go tam nie było. Gdy dwie osoby przekazują sobie kartkę z ręki do ręki, nikt pośrodku nie musi przysięgać, że jej nie przeczytał. Po prostu nie ma nikogo pośrodku.

Większość rzeczy w codziennym życiu działa w ten sposób. Nie podpisujemy umów o zachowaniu poufności z powietrzem, które przenosi nasz głos, ani z papierem, który trzymamy. Prywatność rozmowy nie opiera się na obietnicy pośrednika, ponieważ nie ma pośrednika. To jeden z najsilniejszych sposobów na bycie prywatnym: nie dlatego, że coś lub ktoś zachowuje się dobrze, ale dlatego, że tego czegoś lub kogoś nie ma.

Gdy rozmowa przenosi się do kanału cyfrowego, domyślnie ulega to zmianie. Zazwyczaj model wygląda następująco: dwie osoby łączą się z serwerem, serwer odbiera wiadomość, szyfruje ją lub przechowuje zaszyfrowaną i dostarcza odbiorcy. Serwer jest pośrodku. Serwer może być uczciwy. Może być audytowany. Może działać w sprzyjającej jurysdykcji i zgodnie z surową polityką prywatności. To wszystko może być prawdą. Ale serwer jest pośrodku.

Różnica między szyfrowaniem a niegromadzeniem danych (część druga)

W poprzednim artykule z tej serii twierdziliśmy, że szyfrowanie treści i niegromadzenie metadanych to nie to samo. Warto sformułować jasno kolejny krok: szyfrowanie tego, co przechodzi przez serwer, i brak serwera to również nie to samo.

Pierwszy model — serwer pośrodku, treść zaszyfrowana — chroni treść przed operatorem serwera, jego personelem technicznym oraz zewnętrznym napastnikiem, który mógłby złamać system. I to jest ważne. Ale nie eliminuje serwera. Serwer nadal tam jest. Nadal przetwarza metadane. Nadal jest punktem, który może otrzymać wezwanie sądowe, interwencję prawną, presję polityczną lub doznać naruszenia bezpieczeństwa. Nadal jest punktem wymagającym obdarzenia kogoś zaufaniem.

Drugi model — brak serwera między dwoma końcami — nie chroni lepiej zaszyfrowanej treści: jeśli kryptografia jest solidna, treść jest chroniona w obu przypadkach. Zmienia się nie treść, lecz to, że pytanie *„co dzieje się z serwerem?”* przestaje mieć sens, ponieważ nie ma serwera, o który można by pytać.

Zaufanie, nieobecność i różnica między nimi

Zaufanie może być dobrze ulokowane. Istnieją uczciwe firmy. Istnieją rzetelni audytorzy. Istnieją przepisy sprzyjające użytkownikom. Istnieją poważne usługi, które skrupulatnie przestrzegają powyższych zasad.

Zaufanie, gdy jest udzielane operatorowi, który na nie zasługuje, nie jest złym rozwiązaniem.

Ale zaufanie, bez względu na to, jak solidne, pozostaje tylko zaufaniem. To rozwiązanie społeczne, a nie techniczne. Firma może zmienić właściciela. Jurysdykcja może zmienić rząd. Nakaz sądowy może wpłynąć jutro. Nowa podatność może zostać odkryta w przyszłym miesiącu. Nic z tego nie dzieje się w złej wierze. Dzieje się tak, ponieważ operator istnieje, a wszystko, co istnieje, podlega nieprzewidzianym okolicznościom tego świata.

Nieobecność operatora nie podlega tym samym okolicznościom. Nakaz sądowy nie może żądać danych od serwera, który nie istnieje. Napastnik nie może włamać się na serwer, który nie istnieje. Zmiana polityki firmy nie może wpłynąć na dane, których ta firma nigdy nie miała. Kluczowe zdanie jest proste: danych, które nie istnieją, nie można stracić.

O uzasadnionym argumencie strony serwerowej

Podmioty oferujące profesjonalne usługi komunikacyjne z serwerem pośrodku zazwyczaj formułują trzy w pełni słuszne argumenty. Po pierwsze, że serwer jest niezbędny do zagwarantowania dostarczenia wiadomości, gdy odbiorca jest offline. Po drugie, że szyfrowanie treści jest silne, więc operator nie może jej odczytać. Po trzecie, że usługa jest zgodna z europejskim prawem i dane są chronione przez prawo.

Wszystkie trzy argumenty są prawdziwe. Żaden z nich nie zmienia natury rzeczy. Prawdą jest, że serwer pozwala na przechowywanie wiadomości w celu ich późniejszego dostarczenia; prawdą jest również, że problem ten można rozwiązać inaczej, poprzez protokoły bezpośredniej komunikacji między urządzeniami, dopracowywane od dekad i działające dzisiaj. Prawdą jest, że szyfrowanie treści w tranzycie jest solidne w poważnych usługach. I prawdą jest, że europejskie prawo chroni użytkowników bardziej niż w wielu innych miejscach.

Kwestią nie jest to, czy usługi z serwerem pośrodku są legalne, bezpieczne lub czy chronią treść. Mogą takie być, są legalne i zazwyczaj są bezpieczne. Kwestią jest to, że posiadanie serwera pośrodku to wybór architektoniczny, a nie techniczny wymóg. A każdy wybór ma swoje konsekwencje. Architektura z serwerem pośrodku koniecznie tworzy aktora, któremu trzeba zaufać. Architektura bez serwera pośrodku — nie.

Co mówi prawo, a co robi architektura

RODO nie wymaga konkretnego modelu architektonicznego. Wymaga rezultatów: minimalizacji danych, ograniczenia celu, ochrony danych w fazie projektowania i domyślnej ochrony, zdolności do wykazania zgodności. Usługa z serwerem pośrodku może spełniać wszystkie te wymagania. Usługa bez serwera pośrodku spełnia kilka z nich poprzez samą konstrukcję, a nie deklarację. Absolutna minimalizacja — niegromadzenie niczego, co nie jest ściśle niezbędne do dostarczenia wiadomości — jest trywialna, gdy nie ma serwera, który mógłby cokolwiek zgromadzić.

W przypadku codziennych, niewrażliwych zastosowań architektura serwerowa jest w pełni rozsądna, a zaufanie do poważnego operatora jest poprawnym rozwiązaniem. W przypadku innych zastosowań — objętych tajemnicą zawodową, wiążących się z odpowiedzialnością etyczną, dotyczących szczególnie wrażliwych informacji — brak punktu zaufania nie jest luksusem, lecz przewagą strukturalną.

Dla profesjonalnego czytelnika

Pytania, które warto sobie zadać przed skorzystaniem z profesjonalnej usługi komunikacyjnej, znane już z poprzednich artykułów z tej serii, dopełnia jeszcze jedno pytanie architektoniczne:

1. Czy szyfruje treść w tranzycie? (Prawdopodobnie tak).
2. Czy generuje i przechowuje metadane o tym, z kim i kiedy rozmawiam? (Prawdopodobnie tak).
3. Czy na drodze między moim urządzeniem a urządzeniem odbiorcy znajduje się serwer?

4. Jeśli istnieje: kto go obsługuje, w jakiej jurysdykcji i co musiałoby się stać, aby przekazał dane o mnie?
5. Jeśli nie istnieje: poprzednie pytania stają się bezprzedmiotowe.

Różnica między tymi dwiema kategoriami nie jest kwestią stopnia, lecz rodzaju. Gdy przychodzi czas na wyjaśnienie tego klientowi, pacjentowi lub koledze, najuczciwsza formuła jest zarazem najprostszą: w jednym przypadku ktoś jest pośrodku; w drugim — nie.

Ten artykuł zamyka pierwszy cykl Cuadernos Lacre. Po omówieniu szyfrowania, metadanych i tajemnicy zawodowej dopełniamy obraz architektoniczny: szyfrowanie treści i brak serwera pośrodku to różne rzeczy. Obie mogą być legalne; tylko jedna eliminuje konieczność obdarzania kogoś zaufaniem.

Źródła i dodatkowa lektura

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Fundamentalny tekst o zasadzie, według której gwarancje systemu powinny być wdrażane na jego końcach, a nie w kanale pośrednim.
- Rozporządzenie (UE) 2016/679, art. 25 — ochrona danych w fazie projektowania oraz domyślna ochrona danych.
- Rozporządzenie (UE) 2016/679, art. 5.1.c — zasada minimalizacji danych.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Rozdziały o architekturach minimalizujących gromadzenie danych poprzez samą konstrukcję.

← PoprzedniRODO i komunikacja profesjonalna: dlaczego większość narusza przepisy nie wiedząc o tymNastępny →CUADERNOS_LIST_SCHREMS_TITLE

Ostatnie lektury

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Zabierz ten artykuł tam, gdzie go potrzebujesz.

↓ Markdown ↓ Zwykły tekst ↓ PDF

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczęć lakowa · SHA-256 3bdd5efe4ae36928659d7bcd4dfc0f7b22b87ad615640b7c9c264e38ee781a92

Cuadernos Lacre · Publikacja Menzuri Gestión S.L. ·
napisana przez R.Eugenio · redagowana przez zespół Solo2.