Szyfrowanie to nie prywatność: co mówią o Tobie metadane

Zaszyfrowana treść i widoczne metadane to dwie różne rzeczy. Gdy usługa mówi o "szyfrowaniu end-to-end", opowiada tylko połowę historii.

Kłódka, która nie chroni wszystkiego

Spora część dzisiejszych komunikatorów reklamuje szyfrowanie end-to-end. I to prawda: treść wiadomości podróżuje zaszyfrowana, tak że nikt po drodze – nawet dostawca usługi – nie może odczytać tekstu podczas przesyłania. Do tego momentu stwierdzenie jest dokładne.

Problem w tym, że treść to tylko część historii. Nawet jeśli nikt nie może odczytać tego, co mówisz, usługa wie inne rzeczy z bardzo wysoką precyzją: z kim rozmawiasz, o której godzinie, jak często, z jakiej przybliżonej lokalizacji, na jakim urządzeniu, ile wiadomości wysyłasz i ile odbierasz, ile plików udostępniasz. Wszystko to nazywa się metadanymi. A metadane w wielu przypadkach mówią prawie tyle samo, co sama wiadomość.

Co ujawniają metadane

Nie trzeba czytać wiadomości, aby wiedzieć wiele rzeczy. Jeśli osoba dzwoni lub pisze do onkologa w każdy wtorek o dziewiątej rano przez sześć miesięcy, nie trzeba podsłuchiwać rozmowy, aby domyślić się, co się dzieje. Jeśli dwie osoby wymieniają sto wiadomości dziennie i nagle przestają to robić, nie trzeba czytać żadnej, aby zrozumieć, co się stało. Jeśli doradca podatkowy otrzymuje dwadzieścia wiadomości pod rząd od tego samego klienta w noc przed zamknięciem kwartału, wzorzec mówi sam za siebie.

Metadane ujawniają wzorce zachowań: kto z kim się kontaktuje, jakie kto ma harmonogramy, kiedy nie śpi, kiedy śpi, kiedy podróżuje, którzy klienci są najbardziej aktywni, które relacje zawodowe są najbardziej intensywne. Serwer zbierający metadane może zbudować szczegółowy profil życia osobistego i zawodowego każdego użytkownika, nigdy nie czytając ani jednego słowa z tego, co pisze.

Istnieje historyczny przykład, który dobitnie to ilustruje. Były dyrektor NSA, Michael Hayden, sformułował to bez ogródek w 2014 roku: *"We kill people based on metadata"*. Stwierdzenie odnosiło się do amerykańskich operacji wojskowych przeciwko celom zidentyfikowanym wyłącznie na podstawie wzorców komunikacji. Ani jedna przeczytana wiadomość. Tylko graf kontaktów i godziny.

To, że usługa zbiera metadane, nie oznacza automatycznie, że użyje ich przeciwko swoim użytkownikom. Oznacza to, że ma taką możliwość, i że osoba trzecia mająca dostęp do tych danych – na mocy nakazu sądowego, w wyniku naruszenia bezpieczeństwa lub sprzedaży osobom trzecim, jeśli pozwalają na to warunki usługi – również ją ma.

Dostęp do książki telefonicznej

Inny wektor, który przechodzi niemal niezauważony: lista kontaktów. Spora część komunikatorów prosi o dostęp do książki telefonicznej przy rejestracji. Przesyłają wszystkie numery na swój serwer, aby pokazać, kto jeszcze korzysta z usługi. Od tego momentu firma ma kompletną mapę relacji użytkownika, nawet jeśli ten nigdy do nikogo nie napisał ani jednej wiadomości.

Dla profesjonalisty objętego tajemnicą zawodową – prawnika, lekarza, psychologa, doradcy – ta książka zawiera klientów. Jeśli książka została przesłana na serwer osób trzecich, nazwiska klientów znajdują się w infrastrukturze, nad której jurysdykcją i polityką profesjonalista nie ma kontroli. Tajemnica zawodowa nie zostaje złamana w dniu wycieku rozmowy: została złamana znacznie wcześniej, w momencie wyrażenia zgody na przesłanie.

Różnica między szyfrowaniem a nie-zbieraniem

Szyfrowanie to ochrona treści. Prywatność to nie-zbieranie tego, co nie jest potrzebne. To różne rzeczy, a różnica jest operacyjnie krytyczna. Usługa może doskonale szyfrować wszystkie wiadomości i jednocześnie wiedzieć o swoich użytkownikach prawie wszystko dzięki metadanym. Te dwie rzeczy są w pełni kompatybilne. W rzeczywistości jest to dominujący model biznesowy w branży.

Właściwe pytanie do oceny rzeczywistej prywatności usługi nie brzmi *"czy szyfruje treść?"*. Na to pytanie odpowiedź znana jest od lat. Właściwe pytanie brzmi: *"jakie metadane generuje i gdzie są przechowywane?"*. A przede wszystkim: *"jakich metadanych nie musi generować?"*.

Architektura, która minimalizuje metadane poprzez projekt (privacy by design) – nie poprzez obietnicę, nie poprzez politykę wewnętrzną – jest strukturalnie bardziej prywatna niż architektura, która je zbiera i szyfruje. Ponieważ danych, które nie istnieją, nie można wyciec, sprzedać, wydać na nakaz sądowy ani stracić w wyniku włamania.

Dla czytelnika profesjonalnego

Jeśli Twoja działalność zawodowa wiąże się z zachowaniem tajemnicy, poufności lub po prostu szacunkiem dla informacji osób trzecich, warto zadać sobie pytania w tej kolejności:

1. Czy aplikacja, której używam do komunikacji, szyfruje treść? (Prawdopodobnie tak.)
2. Czy szyfruje metadane? (Prawdopodobnie nie.)
3. Czy generuje metadane, których *nie potrzebuje* do działania? (Prawie na pewno tak.)
4. Gdzie te metadane są przechowywane i pod jaką jurysdykcją? (Prawdopodobnie poza Europejskim Obszarem Gospodarczym.)
5. Czy mój klient lub pacjent wie, że jego dane tam są?

Ostatnie pytanie jest niewygodne. Ponieważ szczera odpowiedź w większości przypadków brzmi: nie.

Ten artykuł jest pierwszym z serii o rzeczywistym działaniu profesjonalnych narzędzi komunikacyjnych. Przyszłe wydania poruszą kwestię zgodności z RODO w komunikatorach oraz koncepcję tajemnicy zawodowej w erze cyfrowej.

Źródła i dodatkowa lektura

- Hayden, M. – Deklaracja na Johns Hopkins University, 2014 ("We kill people based on metadata"). Dostępne publiczne transkrypcje.
- RODO (Rozporządzenie UE 2016/679), art. 4 i 5 – definicja danych osobowych i zasady przetwarzania (metadane są danymi osobowymi).

- EIOD i EORODO – opinie w sprawie przetwarzania danych o ruchu i metadanych w komunikacji elektronicznej (dyrektywa ePrivacy).

← PoprzedniKrótka historia pieczęci lakowejNastępny →Tajemnica zawodowa w erze cyfrowej

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 bda706f805e679ed93bb81751ba3b4ba0ac79f33448d1d76db50e643484083c0

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