A cripta nu înseamnă a avea confidențialitate: ce spun metadatele despre dumneavoastră

Conținutul criptat și metadatele vizibile sunt două lucruri diferite. Când un serviciu vorbește despre „criptare end-to-end”, spune doar jumătate din poveste.

Lacătul care nu protejează totul

O mare parte din serviciile de mesagerie de astăzi fac publicitate criptării end-to-end. Și este adevărat: conținutul mesajelor călătorește criptat, astfel încât nimeni pe parcurs – nici măcar furnizorul de servicii – nu poate citi textul în timp ce acesta este în tranzit. Până aici, afirmația este exactă.

Problema este că conținutul este doar o parte a poveștii. Deși nimeni nu poate citi ceea ce spuneți, serviciul știe alte lucruri cu o precizie foarte mare: cu cine vorbiți, la ce oră, cât de des, din ce locație aproximativă, pe ce dispozitiv, câte mesaje trimiteți și câte primiți, câte fișiere partajați. Toate acestea se numesc metadate. Iar metadatele, în multe cazuri, spun aproape la fel de multe ca și mesajul în sine.

Ce dezvăluie metadatele

Nu este nevoie să citești un mesaj pentru a ști multe lucruri. Dacă o persoană sună sau scrie unui oncolog în fiecare marți dimineață la ora nouă timp de șase luni, nu este necesar să asculți conversația pentru a bănui ce se întâmplă. Dacă două persoane schimbă o sută de mesaje pe zi și dintr-odată se opresc, nu trebuie să citești niciunul pentru a înțelege ce s-a întâmplat. Dacă un consultant fiscal primește douăzeci de mesaje la rând de la același client în noaptea de dinaintea închiderii trimestriale, modelul vorbește de la sine.

Metadatele dezvăluie modele de comportament: cine cu cine este în relație, ce programe are fiecare persoană, când este trează, când doarme, când călătorește, care clienți sunt cei mai activi, care relații profesionale sunt cele mai intense. Un server care colectează metadate poate construi un profil detaliat al vieții personale și profesionale a oricărui utilizator fără a citi vreodată un singur cuvânt din ceea ce scrie.

Există un exemplu istoric care ilustrează acest lucru cu duritate. Fostul director al NSA, Michael Hayden, a formulat-o fără menajamente în 2014: *„We kill people based on metadata”*. Afirmația se referea la operațiunile militare americane împotriva unor ținte identificate exclusiv pe baza modelelor lor de comunicare. Niciun mesaj citit. Doar graful de contacte și orarele.

Faptul că un serviciu colectează metadate nu înseamnă neapărat că le va folosi împotriva utilizatorilor săi. Înseamnă că are capacitatea de a face acest lucru și că o terță parte cu acces la acele date – prin ordin judecătoresc, printr-o breșă de securitate sau prin vânzare către terți, dacă termenii serviciului permit – o are de asemenea.

Accesul la agenda de contacte

Un alt vector care trece aproape neobservat: lista de contacte. O mare parte din serviciile de mesagerie solicită acces la agenda telefonului la înregistrare. Ei încarcă toate numerele pe serverul lor pentru a arăta cine mai folosește serviciul. Din acel moment, compania are o hartă completă a relațiilor utilizatorului, chiar dacă acesta nu a scris niciodată un singur mesaj nimănui.

Pentru un profesionist supus secretului profesional – avocat, medic, psiholog, consultant – acea agendă conține clienți. Dacă agenda a fost încărcată pe un server terț, numele clienților se află într-o infrastructură a cărei jurisdicție și politici profesionistul nu le controlează. Secretul profesional nu este încălcat în ziua în care cineva divulgă o conversație: a fost încălcat mult mai devreme, în momentul acceptării încărcării.

Diferența dintre a cripta și a nu colecta

A cripta înseamnă a proteja conținutul. A avea confidențialitate înseamnă a nu colecta ceea ce nu este necesar. Sunt lucruri diferite, iar diferența este crucială din punct de vedere operativ. Un serviciu poate cripta perfect toate mesajele și, în același timp, poate ști aproape totul despre utilizatorii săi prin intermediul metadatelor. Ambele sunt perfect compatibile. De fapt, este modelul de afaceri dominant în sector.

Întrebarea corectă pentru a evalua confidențialitatea reală a unui serviciu nu este *„criptează conținutul?”*. La această întrebare se răspunde de ani de zile. Întrebarea corectă este: *„ce metadate generează și unde sunt stocate?”*. Și, mai ales: *„ce metadate nu are nevoie să genereze?”*.

O arhitectură care minimizează metadatele prin design – nu prin promisiune, nu prin politică internă – este structural mai privată decât o arhitectură care le colectează și le criptează. Deoarece datele care nu există nu pot fi divulgate, nici vândute, nici predate unui ordin judecătoresc și nici pierdute într-o breșă de securitate.

Pentru cititorul profesionist

Dacă activitatea dumneavoastră profesională implică secretul, confidențialitatea sau pur și simplu respectul față de informațiile terților, merită să vă puneți întrebările în această ordine:

1. Aplicația pe care o folosesc pentru a comunica criptează conținutul? (Probabil da.)
2. Criptează metadatele? (Probabil nu.)
3. Generează metadate de care *nu are nevoie* pentru a funcționa? (Aproape sigur da.)
4. Unde sunt stocate acele metadate și sub ce jurisdicție? (Probabil în afara Spațiului Economic European.)
5. Clientul sau pacientul meu știe că datele sale sunt acolo?

Ultima întrebare este cea inconfortabilă. Pentru că răspunsul onest este, în cele mai multe cazuri: nu.

Acest articol este primul dintr-o serie despre funcționarea reală a instrumentelor de comunicare profesională. Edițiile următoare vor aborda conformitatea cu GDPR în mesagerie și conceptul de secret profesional în era digitală.

Surse și lecturi suplimentare

- Hayden, M. – Declarație la Universitatea Johns Hopkins, 2014 („We kill people based on metadata”). Transcrieri publice disponibile.
- GDPR (Regulamentul UE 2016/679), art. 4 și 5 – definiția datelor cu caracter personal și principiile de prelucrare (metadatele sunt date cu caracter personal).
- EDPS și EDPB – opinii privind prelucrarea datelor de trafic și a metadatelor în comunicațiile electronice (Directiva ePrivacy).

← PrecedentO scurtă istorie a sigiliului de cearăUrmător → Secretul profesional în era digitală

Lecturi recente

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Luați acest articol cu dumneavoastră oriunde aveți nevoie.

↓ Markdown ↓ Text simplu ↓ PDF

Fișierul se va descărca pe dispozitivul dumneavoastră. De acolo îl puteți salva, importa în Solo2 sau partaja oriunde doriți. Cuadernos nu decide destinația în locul dumneavoastră.

Sigiliu de ceară · SHA-256 52868695c67c165dea0e7d867bf91a4a3e024d0a735f8ffe89f523800299667e

Cuadernos Lacre · O publicație a Menzuri Gestión S.L. ·
scrisă de R.Eugenio · editată de echipa Solo2.