Šifriranje nije isto što i privatnost: što metapodaci govore o vama

Šifrirani sadržaj i vidljivi metapodaci dvije su različite stvari. Kada usluga govori o "enkripciji od kraja do kraja", priča samo pola priče.

Lokot koji ne štiti sve

Velik dio današnjih usluga za razmjenu poruka oglašava enkripciju od kraja do kraja. I to je istina: sadržaj poruka putuje šifriran, tako da nitko na putu – čak ni pružatelj usluge – ne može pročitati tekst dok se prenosi. Do te točke, tvrdnja je točna.

Problem je što je sadržaj samo dio priče. Iako nitko ne može pročitati što govorite, usluga zna druge stvari s vrlo visokom preciznošću: s kim razgovarate, u koje vrijeme, koliko često, s koje približne lokacije, na kojem uređaju, koliko poruka šaljete i koliko ih primate, koliko datoteka dijelite. Sve se to naziva metapodacima. A metapodaci u mnogim slučajevima govore gotovo jednako toliko koliko i sama poruka.

Što metapodaci otkrivaju

Ne treba čitati poruku da bi se znale mnoge stvari. Ako osoba šest mjeseci svakog utorka ujutro u devet sati zove ili piše onkologu, ne treba čuti razgovor da bi se naslutilo što se događa. Ako dvije osobe razmijene stotinu poruka dnevno i odjednom prestanu, ne treba pročitati ni jednu da bi se razumjelo što se dogodilo. Ako porezni savjetnik primi dvadeset poruka zaredom od istog klijenta u noći prije kvartalnog zatvaranja, obrazac govori sam za sebe.

Metapodaci otkrivaju obrasce ponašanja: tko je s kim u kontaktu, kakve rasporede ima svaka osoba, kada je budna, kada spava, kada putuje, koji su klijenti najaktivniji, koji su profesionalni odnosi najintenzivniji. Poslužitelj koji prikuplja metapodatke može izgraditi detaljan profil osobnog i profesionalnog života bilo kojeg korisnika, a da nikada ne pročita ni jednu riječ onoga što piše.

Postoji povijesni primjer koji to ilustrira vrlo grubo. Bivši direktor NSA-e, Michael Hayden, uobličio je to bez okolišanja 2014. godine: *"We kill people based on metadata"*. Izjava se odnosila na američke vojne operacije protiv ciljeva identificiranih isključivo na temelju njihovih komunikacijskih obrazaca. Ni jedna pročitana poruka. Samo graf kontakata i rasporedi.

To što usluga prikuplja metapodatke ne znači nužno da će ih upotrijebiti protiv svojih korisnika. To znači da ima tu sposobnost, te da je ima i treća strana s pristupom tim podacima – putem sudskog naloga, zbog sigurnosnog proboja ili prodaje trećim stranama, ako uvjeti usluge to dopuštaju.

Pristup imeniku

Još jedan vektor koji prolazi gotovo nezapaženo: popis kontakata. Velik dio usluga za razmjenu poruka pri registraciji traži pristup imeniku u telefonu. Učitavaju sve brojeve na svoj poslužitelj kako bi pokazali tko još koristi uslugu. Od tog trenutka tvrtka ima potpunu kartu odnosa korisnika, čak i ako taj nikada nikome nije napisao ni jednu poruku.

Za profesionalca s profesionalnom tajnom – odvjetnika, liječnika, psihologa, savjetnika – taj imenik sadrži klijente. Ako je imenik učitan na poslužitelj treće strane, imena klijenata nalaze se u infrastrukturi čiju jurisdikciju i politike profesionalac ne kontrolira. Profesionalna tajna nije prekršena na dan kada netko procuri razgovor: prekršena je mnogo ranije, u trenutku pristanka na učitavanje.

Razlika između šifriranja i neprikupljanja

Šifriranje je zaštita sadržaja. Biti privatan znači ne prikupljati ono što nije potrebno. To su različite stvari i razlika je operativno ključna. Usluga može savršeno šifrirati sve poruke, a istovremeno putem metapodataka znati gotovo sve o svojim korisnicima. Obje su stvari potpuno kompatibilne. Zapravo, to je dominantan poslovni model u industriji.

Pravo pitanje za procjenu stvarne privatnosti usluge nije *"šifrira li sadržaj?"*. Na to pitanje odgovor je poznat godinama. Pravo pitanje glasi: *"koje metapodatke stvara i gdje se pohranjuju?"*. I iznad svega: *"koje metapodatke ne treba stvarati?"*.

Arhitektura koja minimizira metapodatke dizajnom – ne obećanjem, ne internom politikom – strukturno je privatnija od arhitekture koja ih prikuplja i šifrira. Budući da podaci koji ne postoje ne mogu procuriti, prodati se, predati sudskom nalogu niti se izgubiti u proboju.

Za profesionalnog čitatelja

Ako vaše profesionalno djelovanje uključuje tajnu, povjerljivost ili jednostavno poštovanje informacija trećih strana, vrijedi postaviti pitanja ovim redom:

1. Šifrira li aplikacija koju koristim za komunikaciju sadržaj? (Vjerojatno da.)
2. Šifrira li metapodatke? (Vjerojatno ne.)
3. Stvara li metapodatke koji joj za rad *nisu potrebni*? (Gotovo sigurno da.)
4. Gdje su ti metapodaci pohranjeni i pod kojom jurisdikcijom? (Vjerojatno izvan Europskog gospodarskog prostora.)
5. Zna li moj klijent ili pacijent da su njegovi podaci tamo?

Posljednje pitanje je neugodno. Jer iskren odgovor je u većini slučajeva: ne.

Ovaj je članak prvi u nizu o stvarnom radu profesionalnih komunikacijskih alata. Buduća izdanja bavit će se usklađenošću s GDPR-om u razmjeni poruka i konceptom profesionalne tajne u digitalnom dobu.

Izvori i dodatno štivo

- Hayden, M. – Izjava na Sveučilištu Johns Hopkins, 2014. ("We kill people based on metadata"). Dostupni javni transkripti.
- GDPR (Uredba EU 2016/679), čl. 4. i 5. – definicija osobnih podataka i načela obrade (metapodaci su osobni podaci).
- EDPS i EDPB – mišljenja o obradi prometnih podataka i metapodataka u elektroničkim komunikacijama (ePrivacy direktiva).

← PrethodnoKratka povijest voštanog pečataSljedeće →Profesionalna tajna u digitalnom dobu

Nedavna čitanja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ponesite ovaj članak sa sobom gdje god vam zatreba.

↓ Markdown ↓ Obični tekst ↓ PDF

Datoteka će se preuzeti na vaš uređaj. Od tamo je možete spremiti, uvesti u Solo2 ili dijeliti gdje god želite. Cuadernos ne odlučuje o odredištu umjesto vas.

Voštani pečat · SHA-256 8fa4f7173e00a3d7cf67b432c7d3c8a24cd163b5550c3c52f9001906317f0917

Cuadernos Lacre · Publikacija Menzuri Gestión S.L. ·
napisao R.Eugenio · uredio tim Solo2.