Analiza · 16. maj 2026

← Prejšnji·Naslednji →

Šifriranje ni isto kot zasebnost: kaj o vas povedo metapodatki

Šifrirana vsebina in vidni metapodatki sta dve različni stvari. Ko storitev govori o "šifriranju od konca do konca", pove le polovico zgodbe.

Ključavnica, ki ne ščiti vsega

Velik del današnjih storitev za sporočanje oglašuje šifriranje od konca do konca. In to je res: vsebina sporočil potuje šifrirano, tako da nihče na poti – niti ponudnik storitve – ne more prebrati besedila, medtem ko se prenaša. Do te točke je trditev natančna.

Težava je v tem, da je vsebina le del zgodbe. Čeprav nihče ne more prebrati, kaj pravite, storitev ve druge stvari z zelo visoko natančnostjo: s kom govorite, ob kateri uri, kako pogosto, s katere približne lokacije, na kateri napravi, koliko sporočil pošljete in koliko jih prejmete, koliko datotek delite. Vse to se imenuje metapodatki. In metapodatki v mnogih primerih povedo skoraj toliko kot samo sporočilo.

Kaj razkrivajo metapodatki

Ni treba prebrati sporočila, da bi vedeli veliko stvari. Če oseba šest mesecev vsak torek zjutraj ob devetih pokliče ali piše onkologu, ni treba slišati pogovora, da bi uganili, kaj se dogaja. Če dve osebi izmenjata sto sporočil na dan in nenadoma prenehata, ni treba prebrati niti enega, da bi razumeli, kaj se je zgodilo. Če davčni svetovalec prejme dvajset sporočil zapored od iste stranke v noči pred četrtletnim zaprtjem, vzorec govori sam zase.

Metapodatki razkrivajo vzorce vedenja: kdo je v stiku s kom, kakšne urnike ima vsaka oseba, kdaj je budna, kdaj spi, kdaj potuje, katere stranke so najbolj aktivne, kateri poslovni odnosi so najbolj intenzivni. Strežnik, ki zbira metapodatke, lahko zgradi podroben profil osebnega in poklicnega življenja katerega koli uporabnika, ne da bi kdaj prebral eno samo besedo tistega, kar piše.

Obstaja zgodovinski primer, ki to ponazarja zelo trdo. Nekdanji direktor NSA, Michael Hayden, je to leta 2014 ubesedil brez ovinkarjenja: *"We kill people based on metadata"*. Izjava se je nanašala na ameriške vojaške operacije proti ciljem, identificiranim izključno na podlagi njihovih komunikacijskih vzorcev. Niti eno prebrano sporočilo. Samo graf kontaktov in urniki.

To, da storitev zbira metapodatke, ne pomeni nujno, da jih bo uporabila proti svojim uporabnikom. Pomeni, da ima to sposobnost in da jo ima tudi tretja oseba z dostopom do teh podatkov – na podlagi sodnega naloga, zaradi varnostne kršitve ali prodaje tretjim osebam, če pogoji storitve to dopuščajo.

Dostop do imenika

Še en vektor, ki ostane skoraj neopažen: seznam kontaktov. Velik del storitev za sporočanje ob registraciji prosi za dostop do imenika v telefonu. Vse številke naložijo na svoj strežnik, da pokažejo, kdo še uporablja storitev.

Od tistega trenutka ima podjetje popoln zemljevid uporabnikovih odnosov, čeprav ta nikoli ni nikomur napisal niti enega sporočila.

Za strokovnjaka s poklicno skrivnostjo – odvetnika, zdravnika, psihologa, svetovalca – ta imenik vsebuje stranke. Če je bil imenik naložen na strežnik tretje osebe, so imena strank v infrastrukturi, katere jurisdikcije in politike strokovnjak ne nadzoruje. Poklicna skrivnost ni prekršena na dan, ko nekdo razkrije pogovor: prekršena je bila že veliko prej, v trenutku privolitve v prenos.

Razlika med šifriranjem in ne-zbiranjem

Šifriranje pomeni zaščito vsebine. Biti zaseben pomeni ne zbirati tistega, kar ni potrebno. To so različne stvari in razlika je operativno ključna. Storitev lahko popolnoma šifrira vsa sporočila in hkrati prek metapodatkov ve skoraj vse o svojih uporabnikih. Obe stvari sta popolnoma združljivi. Dejansko je to prevladujoč poslovni model v panogi.

Pravo vprašanje za oceno dejanske zasebnosti storitve ni *"ali šifrira vsebino?"*. Na to vprašanje je odgovor že leta znan. Pravo vprašanje je: *"katere metapodatke ustvarja in kje so shranjeni?"*. In predvsem: *"katerih metapodatkov ji ni treba ustvarjati?"*.

Arhitektura, ki minimizira metapodatke z zasnovo – ne z obljubo, ne z notranjo politiko – je strukturno bolj zasebna kot arhitektura, ki jih zbira in šifrira. Ker podatki, ki ne obstajajo, ne morejo priti v javnost, se prodati, predati sodnemu nalogu ali izgubiti ob vdoru.

Za profesionalnega bralca

Če vaše poklicno delovanje vključuje skrivnost, zaupnost ali preprosto spoštovanje informacij tretjih oseb, si je vredno zastaviti vprašanja v tem vrstnem redu:

1. Ali aplikacija, ki jo uporabljam za komunikacijo, šifrira vsebino? (Verjetno da.)
2. Ali šifrira metapodatke? (Verjetno ne.)
3. Ali ustvarja metapodatke, ki jih za delovanje *ne potrebuje*? (Skoraj zagotovo da.)
4. Kje so ti metapodatki shranjeni in pod katero jurisdikcijo? (Verjetno zunaj Evropskega gospodarskega prostora.)
5. Ali moja stranka ali pacient ve, da so njeni podatki tam?

Zadnje vprašanje je neprijetno. Ker je iskren odgovor v večini primerov ne.

Ta članek je prvi v seriji o dejanskem delovanju profesionalnih komunikacijskih orodij. Prihodnje številke bodo obravnavale skladnost z GDPR pri sporočanju in koncept poklicne skrivnosti v digitalni dobi.

Viri in nadaljnje branje

- Hayden, M. – Izjava na univerzi Johns Hopkins, 2014 ("We kill people based on metadata"). Na voljo javni prepisi.
- GDPR (Uredba EU 2016/679), čl. 4 in 5 – opredelitev osebnih podatkov in načela obdelave (metapodatki so osebni podatki).
- EDPS in EDPB – mnenja o obdelavi prometnih podatkov in metapodatkov v elektronskih komunikacijah (direktiva o e-zasebnosti).

← PrejšnjiKratka zgodovina voščenega pečataNaslednji →Poklicna skrivnost v digitalni dobi

Zadnja branja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vzemite ta članek s seboj, kamor koli ga potrebujete.

↓ Markdown ↓ Navadno besedilo ↓ PDF

Datoteka bo prenesena v vašo napravo. Od tam jo lahko shranite, uvozite v Solo2 ali delite, kjer koli želite. Cuadernos ne odloča o cilju namesto vas.

Voščeni pečat · SHA-256 03dfe72685fbdc3d236e506fe886da0edf9d6e02a57eacc83e9fcf4310522f68

Cuadernos Lacre · Publikacija podjetja Menzuri Gestión S.L. ·
napisal R.Eugenio · uredila ekipa Solo2.