Analīze · 2026. gada 16. maijs

← Iepriekšējais · Nākamais →

Šifrēt nenozīmē būt privātam: ko par jums saka metadati

Šifrēts saturs un redzami metadati ir divas dažādas lietas. Kad dienests runā par „pilnīgu šifrēšanu”, tas stāsta tikai pusi stāsta.

Slēdzene, kas neaizsargā visu

Liela daļa mūsdienu ziņapmaiņas dienestu reklamē pilnīgu šifrēšanu. Un tā ir taisnība: ziņu saturs ceļo aizšifrēts, tā ka neviens pa ceļam – pat ne pakalpojumu sniedzējs – nevar izlasīt tekstu tā pārsūtīšanas laikā. Līdz šim apgalvojums ir precīzs.

Problēma ir tā, ka saturs ir tikai daļa stāsta. Lai gan neviens nevar izlasīt to, ko jūs sakāt, dienests zina citas lietas ar ļoti augstu precizitāti: ar ko jūs runājat, kurā stundā, cik bieži, no kādas aptuvenas atrašanās vietas, kādā ierīcē, cik ziņu sūtāt un cik saņemat, cik failu kopīgojat. To visu sauc par metadatiem. Un metadati daudzos gadījumos saka gandrīz tikpat daudz cik pati ziņa.

Ko atklāj metadati

Nav jālasa ziņa, lai zinātu daudzas lietas. Ja persona sešus mēnešus katru otrdienas rītu pulksten deviņos zvana vai raksta onkologam, nav nepieciešams dzirdēt sarunu, lai nojaustu, kas notiek. Ja divas personas dienā apmainās ar simts ziņām un pēkšņi pārstāj to darīt, nav jālasa neviena, lai saprastu, kas ir noticis. Ja nodokļu konsultants saņem divdesmit ziņas pēc kārtas no tā paša klienta naktī pirms ceturkšņa noslēguma, modelis runā pats par sevi.

Metadati atklāj uzvedības modeļus: kurš ar kuru ir attiecībās, kādi ir katras personas grafiki, kad viņi ir nomodā, kad guļ, kad ceļo, kuri klienti ir visaktīvākie, kuras profesionālās attiecības ir visintensīvākās. Serveris, kas vāc metadatus, var izveidot detalizētu jebkura lietotāja personīgās un profesionālās dzīves profilu, nekad neizlasot ne vārda no tā, ko viņš raksta.

Ir vēsturisks piemērs, kas to ilustrē ļoti skarbi. Bijušais NSA direktors Maikls Heidens (Michael Hayden) to tieši noformulēja 2014. gadā: *„We kill people based on metadata”*. Apgalvojums attiecās uz ASV militārajām operācijām pret mērķiem, kas identificēti vienīgi pēc to komunikācijas modeļiem. Neviena izlasīta ziņa. Tikai kontaktu grafs un grafiki.

Tas, ka dienests vāc metadatus, nenozīmē obligāti, ka tas tos izmantos pret saviem lietotājiem. Tas nozīmē, ka tam ir šāda iespēja un ka trešajai pusei ar piekļuvi tiem datiem – saskaņā ar tiesas rīkojumu, drošības pārkāpuma dēļ vai pārdodot trešajām pusēm, ja pakalpojuma sniegšanas noteikumi to pieļauj – tā ir arī.

Piekļuve kontaktu grāmatai

Cits vektors, kas paliek gandrīz nepamanīts: kontaktu saraksts. Liela daļa ziņapmaiņas dienestu reģistrējoties prasa piekļuvi tālruņa kontaktu grāmatai. Viņi augšupielādē visus numurus savā serverī, lai parādītu, kurš vēl izmanto dienestu. No tā brīža uzņēmumam ir pilna lietotāja attiecību karte, pat ja tas nekad nevienam nav uzrakstījis nevienu ziņu.

Profesionālim, kas glabā profesionālo noslēpumu – advokātam, ārstam, psihologam, konsultantam – tajā kontaktu grāmatā ir klienti. Ja kontaktu grāmata tika augšupielādēta trešās puses serverī, klientu uzvārdi atrodas infrastruktūrā, kuras jurisdikciju un politikas profesionālis nekontrolē. Profesionālais noslēpums netiek pārkāpts tajā dienā, kad kāds nopludina sarunu: tas tika pārkāpts daudz agrāk, augšupielādes piekrišanas brīdī.

Atšķirība starp šifrēšanu un nevākšanu

Šifrēt nozīmē aizsargāt saturu. Būt privātam nozīmē nevākt to, kas nav nepieciešams. Tās ir dažādas lietas, un atšķirība ir operatīvi izšķiroša. Dienests var perfekti aizšifrēt visas ziņas un tajā pašā laikā caur metadatiem zināt gandrīz visu par saviem lietotājiem. Abi divi ir pilnīgi saderīgi. Patiesībā tas ir dominējošais biznesa modelis nozarē.

Pareizais jautājums, lai novērtētu dienesta patieso privātumu, nav *„vai tas šifrē saturu?”*. Uz šo jautājumu ir atbildēts jau gadiem. Pareizais jautājums ir: *„kādus metadatus tas ģenerē un kur tie tiek glabāti?”*. Un, galvenais: *„kādus metadatus tam nevajadzētu ģenerēt?”*.

Arhitektūra, kas minimizē metadatus pēc konstrukcijas (privacy by design) – nevis pēc solījuma, nevis pēc iekšējās politikas –, ir strukturāli privātāka nekā arhitektūra, kas tos vāc un šifrē. Tāpēc ka dati, kuru nav, nevar tikt nopludināti, pārdoti, nodoti saskaņā ar tiesas rīkojumu vai pazaudēti drošības pārkāpumā.

Profesionālajam lasītājam

Ja jūsu profesionālā darbība ietver noslēpumu, konfidencialitāti vai vienkārši cieņu pret trešo pušu informāciju, ir vērts uzdot jautājumus šādā secībā:

1. Vai lietotne, ko izmantoju komunikācijai, šifrē saturu? (Droši vien jā.)
2. Vai tā šifrē metadatus? (Droši vien nē.)
3. Vai tā ģenerē metadatus, kas tai *nav nepieciešami* darbībai? (Gandrīz noteikti jā.)
4. Kur tiek glabāti tie metadati un kādā jurisdikcijā? (Droši vien ārpus Eiropas Ekonomikas zonas.)
5. Vai mans klients vai pacients zina, ka viņa dati ir tur?

Pēdējais jautājums ir tas nepatīkamais. Tāpēc ka godīgā atbilde vairumā gadījumu ir: nē.

Šis raksts ir pirmais no sērijas par profesionālo komunikācijas rīku patieso darbību. Nākamie numuri pievērsīsies VDAR atbilstībai ziņapmaiņā un profesionālā noslēpuma koncepcijai digitālajā laikmetā.

Avoti un papildu literatūra

- Hayden, M. – Deklarācija Džonsa Hopkinsa universitātē, 2014. gadā („We kill people based on metadata”). Pieejamas publiskas transkripcijas.
- VDAR (ES regula 2016/679), 4. un 5. pants – personas datu definīcija un apstrādes principi (metadati ir personas dati).
- EDAU un EDPB – atzinumi par satiksmes datu un metadatu apstrādi elektroniskajā komunikācijā („e-privātuma” direktīva).

← IepriekšējaisĪsa vaska zīmoga vēstureNākamais →Profesionālais noslēpums digitālajā laikmetā

Jaunākie lasījumi

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Paņemiet šo rakstu līdzi tur, kur jums nepieciešams.

↓ Markdown ↓ Parasts teksts ↓ PDF

Fails tiks lejupielādēts jūsu ierīcē. No turienes varat to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi jūsu vietā.

Vaska zīmogs · SHA-256 5220c7cf823dd03c4db2b57275410b2db2d5fb44bd02de98073148422ea313e3

Cuadernos Lacre · Menzuri Gestión S.L. publikācija ·
autors R.Eugenio · rediģējusi Solo2 komanda.