Analizė · 2026 m. gegužės 16 d.

← Ankstesnis·Kitas →

Šifruoti nereiškia būti privačiam: ką apie jus sako metaduomenys

Užšifruotas turinys ir matomi metaduomenys yra du skirtingi dalykai. Kai paslauga kalba apie „ištisinį šifravimą“, ji pasakoja tik pusę istorijos.

Spyna, kuri neapsaugo visko

Didelė dalis šiuolaikinių susirašinėjimo paslaugų reklamuoja ištisinį šifravimą. Ir tai tiesa: žinučių turinys keliauja užšifruotas, todėl niekas pakeliui – net paslaugų teikėjas – negali perskaityti teksto, kol jis perduodamas. Iki šiol teiginys yra tikslus.

Problema ta, kad turinys yra tik dalis istorijos. Nors niekas negali perskaityti to, ką sakote, paslauga žino kitus dalykus labai dideliu tikslumu: su kuo kalbate, kurią valandą, kaip dažnai, iš kokios apytikslės vietos, kokiame įrenginyje, kiek žinučių siunčiate ir kiek gaunate, kiek failų bendrinate. Visa tai vadinama metaduomenimis. O metaduomenys daugeliu atvejų sako beveik tiek pat, kiek ir pati žinutė.

Ką atskleidžia metaduomenys

Nereikia skaityti žinutės, kad žinotum daug dalykų. Jei asmuo skambina arba rašo onkologui kiekvieną antradienio rytą devintą valandą šešis mėnesius, nebūtina girdėti pokalbio, kad nuspėtum, kas vyksta. Jei du asmenys per dieną pasikeičia šimtu žinučių ir staiga nustoja tai daryti, nereikia skaityti nei vienos, kad suprastum, kas nutiko. Jei mokesčių konsultantas gauna dvidešimt žinučių iš eilės iš to paties kliento naktį prieš ketvirčio pabaigą, modelis kalba pats už save.

Metaduomenys atskleidžia elgsenos modelius: kas su kuo palaiko santykius, kokie yra kiekvieno asmens tvarkaraščiai, kada jie pabudę, kada miega, kada keliauja, kurie klientai yra aktyviausi, kurie profesiniai santykiai yra intensyviausi. Metaduomenis renkantis serveris gali sukurti išsamų bet kurio vartotojo asmeninio ir profesinio gyvenimo profilį, niekada neperskaitęs nei vieno jo rašomo žodžio.

Yra istorinis pavyzdys, kuris tai iliustruoja labai griežtai. Buvęs NSA direktorius Michael Hayden tai tiesiai suformulavo 2014 m.: *„We kill people based on metadata“*. Teiginys nurodė į JAV karines operacijas prieš taikinius, identifikuotus išimtinai pagal jų komunikacijos modelius. Nei vienos perskaitytos žinutės. Tik kontaktų grafas ir tvarkaraščiai.

Tai, kad paslauga renka metaduomenis, nebūtinai reiškia, kad ji juos naudos prieš savo vartotojus. Tai reiškia, kad ji turi tam galimybę, ir kad trečioji šalis, turinti prieigą prie tų duomenų – pagal teismo sprendimą, dėl saugumo pažeidimo ar pardavimo trečiosioms šalims, jei paslaugų teikimo sąlygos tai leidžia – taip pat ją turi.

Prieiga prie kontaktų knygos

Kitas vektorius, kuris lieka beveik nepastebėtas: kontaktų sąrašas. Didelė dalis susirašinėjimo paslaugų registruojantis prašo prieigos prie telefono kontaktų knygos. Jie įkelia visus numerius į savo serverį, kad parodytų, kas dar naudojasi paslauga. Nuo tos akimirkos įmonė turi pilną vartotojo santykių žemėlapį, net jei jis niekada niekam neparašė nei vienos žinutės.

Profesionalui, saugančiam profesinę paslaptį – advokatui, gydytojui, psichologui, konsultantui – toje kontaktų knygoje yra klientai. Jei kontaktų knyga buvo įkelta į trečiosios šalies serverį, klientų pavardės yra infrastruktūroje, kurios jurisdikcijos ir politikos profesionalas nekontroliuoja. Profesinė paslaptis nėra pažeidžiama tą dieną, kai kas nors nutekina pokalbį: ji buvo pažeista daug anksčiau, įkėlimo sutikimo momentu.

Skirtumas tarp šifravimo ir nerinkimo

Šifruoti reiškia saugoti turinį. Būti privačiam reiškia nerrinkti to, ko nereikia. Tai skirtingi dalykai, ir skirtumas yra operatyviai lemiamas. Paslauga gali puikiai šifruoti visas žinutes ir tuo pačiu metu per metaduomenis žinoti beveik viską apie savo vartotojus. Abu dalykai yra visiškai suderinami. Tiesą sakant, tai yra dominuojantis verslo modelis sektoriuje.

Teisingas klausimas norint įvertinti tikrąjį paslaugos privatumą nėra *„ar ji šifruoja turinį?“*. Į šį klausimą atsakyta jau prieš kelerius metus. Teisingas klausimas yra: *„kokius metaduomenis ji generuoja ir kur jie saugomi?“*. Ir, svarbiausia: *„kokių metaduomenų jai nereikia generuoti?“*.

Architektūra, kuri minimizuoja metaduomenis pagal projektą (privacy by design) – ne pagal pažadą, ne pagal vidinę politiką – yra struktūriškai privatesnė nei architektūra, kuri juos renka ir šifruoja. Nes duomenys, kurių nėra, negali būti nutekinti, parduoti, perduoti pagal teismo sprendimą ar prarasti per saugumo pažeidimą.

Profesionaliam skaitytojui

Jei jūsų profesinė veikla apima paslaptį, konfidencialumą ar tiesiog pagarbą trečiųjų šalių informacijai, verta užduoti klausimus šia tvarka:

1. Ar programėlė, kurią naudoju komunikacijai, šifruoja turinį? (Tikriausiai taip.)
2. Ar ji šifruoja metaduomenis? (Tikriausiai ne.)
3. Ar ji generuoja metaduomenis, kurių jai *nereikia* veikimui? (Beveik neabejotinai taip.)
4. Kur saugomi tie metaduomenys ir kokioje jurisdikcijoje? (Tikriausiai už Europos ekonominės erdvės ribų.)
5. Ar mano klientas ar pacientas žino, kad jo duomenys yra ten?

Paskutinis klausimas yra nemalonus. Nes sąžiningas atsakymas daugeliu atvejų yra: ne.

Šis straipsnis yra pirmasis iš serijos apie tikrąjį profesionalių komunikacijos įrankių veikimą. Būsimuose numeriuose bus nagrinėjamas BDAR laikymasis susirašinėjimo programėlėse ir profesinės paslapties koncepcija skaitmeniniame amžiuje.

Šaltiniai ir papildomas skaitymas

- Hayden, M. – Deklaracija Johns Hopkins universitete, 2014 m. („We kill people based on metadata“). Prieinamos viešos transkripcijos.
- BDAR (ES reglamentas 2016/679), 4 ir 5 str. – asmens duomenų apibrėžimas ir tvarkymo principai (metaduomenys yra asmens duomenys).
- EDAPP ir EDPB – nuomonės dėl srauto duomenų ir metaduomenų tvarkymo elektroninių ryšių srityje („e. privatumo“ direktyva).

← AnkstesnisTrumpa vaško antspaudo istorijaKitas →Profesinė paslaptis skaitmeniniame amžiuje

Naujausi skaitiniai

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Pasiimkite šį straipsnį su savimi ten, kur jums reikia.

↓ Markdown ↓ Paprastas tekstas ↓ PDF

Failas bus atsisiųstas į jūsų įrenginį. Iš ten galite jį išsaugoti, importuoti į Solo2 arba bendrinti bet kur. Cuadernos nusprendžia ne jūsų naudai dėl paskirties vietos.

Vaško antspaudas · SHA-256 5b76510c34572ffaa799faf92985db3651f534375936a1141d43fd5cb8ea77fc

Cuadernos Lacre · Menzuri Gestión S.L. leidinys ·
parašė R.Eugenio · redagavo Solo2 komanda.

Ši svetainė nenaudoja slapukų ir neįkelia trečiųjų šalių išteklių. Ji naudoja savarankiškai priglobtą anoniminį lankytojų skaitiklį (Umami, mūsų Europos serveryje) ir minimalų JavaScript kiekį, būtiną jūsų šviesios/tamsios temos pasirinkimui. Jokių seklių, jokio profiliavimo, jokio dalijimosi duomenimis. Jei norite mus sekti: RSS.