Šifrovať neznamená byť v súkromí: čo o vás vypovedajú metadáta

Šifrovaný obsah a viditeľné metadáta sú dve odlišné veci. Keď služba hovorí o "koncovom šifrovaní", rozpráva len polovicu príbehu.

Zámok, ktorý nechráni všetko

Veľká časť dnešných messagingových služieb inzeruje koncové šifrovanie. A je to pravda: obsah správ putuje šifrovane, takže nikto na ceste – dokonca ani poskytovateľ služby – nemôže text počas prenosu čítať. Potiaľ je tvrdenie presné.

Problém je, že obsah je len časťou príbehu. Aj keď nikto nemôže čítať, čo hovoríte, služba pozná iné veci s veľmi vysokou presnosťou: s kým hovoria, v koľkej hodine, ako často, z akej približnej polohy, na akom zariadení, koľko správ odosielate a koľko prijímate, koľko súborov zdieľate. Tomu všetkému sa hovorí metadáta. A metadáta v mnohých prípadoch vypovedajú takmer toľko ako samotná správa.

Čo metadáta odhaľujú

Nie je potrebné čítať správu, aby sme vedeli veľa vecí. Ak niekto volá alebo píše onkológovi každý utorok o deviatej ráno po dobu šiestich mesiacov, nie je nutné počúvať rozhovor, aby sme tušili, čo sa deje. Ak si dvaja ľudia vymenia sto správ denne a zrazu s tým prestanú, netreba čítať žiadnu, aby sme pochopili, čo sa stalo. Ak daňový poradca dostane dvadsať správ v rade od toho istého klienta noc pred štvrťročnou uzávierkou, vzorec hovorí sám za seba.

Metadáta odhaľujú vzorce správania: kto sa s kým stýka, aký má kto rozvrh, kedy bdie, kedy spí, kedy cestuje, ktorí klienti sú najaktívnejší, ktoré profesijné vzťahy sú najintenzívnejšie. Server, ktorý zbiera metadáta, môže zostaviť podrobný profil osobného aj profesijného života ktoréhokoľvek používateľa bez toho, aby kedy prečítal jediné slovo z toho, čo dotyčný píše.

Existuje historický príklad, ktorý to ilustruje veľmi tvrdo. Bývalý riaditeľ NSA Michael Hayden to v roku 2014 formuloval bez obalu: *"We kill people based on metadata"*. Tvrdenie sa týkalo amerických vojenských operácií proti cieľom identifikovaným výhradne na základe ich komunikačných vzorcov. Ani jedna prečítaná správa. Iba graf kontaktov a časové údaje.

To, že služba zbiera metadáta, neznamená nutne, že ich použije proti svojim používateľom. Znamená to, že k tomu má schopnosť a že tretia strana s prístupom k týmto údajom – na základe súdneho príkazu, v dôsledku narušenia bezpečnosti alebo predaja tretím stranám, ak to podmienky služby umožňujú – ju má tiež.

Prístup ku kontaktom

Ďalší vektor, ktorý prechádza takmer bez povšimnutia: zoznam kontaktov. Veľká časť messagingových služieb žiada pri registrácii o prístup k telefónnemu zoznamu. Nahrajú všetky čísla na svoj server, aby ukázali, kto ďalší službu používa. Od tej chvíle má spoločnosť kompletnú mapu vzťahov používateľa, aj keď ten nikdy nikomu nenapísal jedinú správu.

Pre profesionála s profesijným tajomstvom – právnika, lekára, psychológa, poradcu – tento zoznam obsahuje klientov. Ak bol zoznam nahraný na server tretej strany, mená klientov sú v infraštruktúre, ktorej jurisdikciu a politiku profesionál nekontroluje. Profesijné tajomstvo sa neporuší v deň úniku konverzácie: bolo porušené oveľa skôr, v okamihu súhlasu s nahraním.

Rozdiel medzi šifrovaním a nezbieraním

Šifrovať znamená chrániť obsah. Byť v súkromí znamená nezbierať to, čo nie je potrebné. Sú to odlišné veci a rozdiel je operačne kritický. Služba môže všetky správy dokonale šifrovať a zároveň o svojich používateľoch vedieť takmer všetko prostredníctvom metadát. Obe veci sú dokonale kompatibilné. V skutočnosti je to dominantný obchodný model v odvetví.

Správna otázka na posúdenie skutočného súkromia služby neznie *"šifruje obsah?"*. Táto otázka je považovaná za zodpovedanú už roky. Správna otázka znie: *"aké metadáta generuje a kde sa ukladajú?"*. A predovšetkým: *"aké metadáta nepotrebuje generovať?"*.

Architektúra, ktorá minimalizuje metadáta zámerne (by design) – nie sľubom, nie internou politikou – je štrukturálne súkromnejšia než architektúra, ktorá ich zbiera a šifruje. Pretože údaje, ktoré neexistujú, nemôžu uniknúť, predať sa, vydať na súdny príkaz ani stratiť pri narušení bezpečnosti.

Pre profesionálneho čitateľa

Ak vaša profesijná činnosť zahŕňa tajomstvo, dôvernosť alebo jednoducho rešpekt k informáciám tretích strán, je vhodné si položiť otázky v tomto poradí:

1. Šifruje aplikácia, ktorú používam na komunikáciu, obsah? (Pravdepodobne áno.)
2. Šifruje metadáta? (Pravdepodobne nie.)
3. Generuje metadáta, ktoré ku svojmu fungovaniu *nepotrebuje*? (Takmer určite áno.)
4. Kde sú tieto metadáta uložené a pod akou jurisdikciou? (Pravdepodobne mimo Európskeho hospodárskeho priestoru.)
5. Vie môj klient alebo pacient, že sú tam jeho údaje?

Posledná otázka je tá nepríjemná. Pretože úprimná odpoveď vo väčšine prípadov znie, že nie.

Tento článok je prvý zo série o skutočnom fungovaní profesionálnych komunikačných nástrojov. Budúce časti sa budú venovať súladu s GDPR v messagingu a konceptu profesijného tajomstva v digitálnej ére.

Zdroje a ďalšie čítanie

- Hayden, M. – Vyhlásenie na Johns Hopkins University, 2014 ("We kill people based on metadata"). Verejné prepisy k dispozícii.
- GDPR (Nariadenie EÚ 2016/679), čl. 4 a 5 – definícia osobných údajov a zásady spracúvania (metadáta sú osobné údaje).
- EDPS a EDPB – stanoviská k spracúvaniu prevádzkových údajov a metadát v elektronických komunikáciách (smernica ePrivacy).

← PredchádzajúciStručná história voskovej pečateNasledujúci →Profesijné tajomstvo v digitálnej ére

Nedávne čítanie

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vezmite si tento článok tam, kam potrebujete.

↓ Markdown ↓ Čistý text ↓ PDF

Súbor sa stiahne do vášho zariadenia. Odtiaľ si ho môžete uložiť, importovať do Solo2 alebo zdieľať, kdekoľvek chcete. Cuadernos za vás o cieli nerozhoduje.

Vosková pečať · SHA-256 04dacfbecb256d2b0275068a236f816beef802c68d7aeb87da8c6eed2b8c5c6b

Cuadernos Lacre · Publikácia spoločnosti Menzuri Gestión S.L. ·
napísal R.Eugenio · edituje tím Solo2.