Šifrovat neznamená být v soukromí: co o vás vypovídají metadata

Šifrovaný obsah a viditelná metadata jsou dvě odlišné věci. Když služba mluví o "koncovém šifrování", vypráví jen polovinu příběhu.

Zámek, který nechrání vše

Velká část dnešních messagingových služeb inzeruje koncové šifrování. A je to pravda: obsah zpráv putuje šifrovaně, takže nikdo na cestě – dokonce ani poskytovatel služby – nemůže text během přenosu číst. Potud je tvrzení přesné.

Problém je, že obsah je jen částí příběhu. I když nikdo nemůže číst, co říkáte, služba zná jiné věci s velmi vysokou přesností: s kým mluvíte, v kolik hodin, jak často, z jaké přibližné polohy, na jakém zařízení, kolik zpráv odesíláte a kolik přijímáte, kolik souborů sdílíte. Tomu všemu se říká metadata. A metadata v mnoha případech vypovídají téměř tolik jako samotná zpráva.

Co metadata odhalují

Není třeba číst zprávu, abychom věděli mnoho věcí. Pokud někdo volá nebo píše onkologovi každé úterý v devět ráno po dobu šesti měsíců, není nutné poslouchat rozhovor, abychom tušili, co se děje. Pokud si dva lidé vymění sto zpráv denně a najednou s tím přestanou, není třeba číst žádnou, abychom pochopili, co se stalo. Pokud daňový poradce obdrží dvacet zpráv v řadě od stejného klienta noc před čtvrtletní uzávěrkou, vzorec mluví sám za sebe.

Metadata odhalují vzorce chování: kdo se s kým stýká, jaký má kdo rozvrh, kdy bdí, kdy spí, kdy cestuje, kteří klienti jsou nejaktivnější, které profesní vztahy jsou nejintenzivnější. Server, který sbírá metadata, může sestavit podrobný profil osobního i profesního života kteréhokoli uživatele, aniž by kdy přečetl jediné slovo z toho, co dotyčný píše.

Existuje historický příklad, který to ilustruje velmi tvrdě. Bývalý ředitel NSA Michael Hayden to v roce 2014 formuloval bez obalu: *"We kill people based on metadata"*. Tvrzení se týkalo amerických vojenských operací proti cílům identifikovaným výhradně na základě jejich komunikačních vzorců. Ani jedna přečtená zpráva. Pouze graf kontaktů a časové údaje.

To, že služba sbírá metadata, neznamená nutně, že je použije proti svým uživatelům. Znamená to, že k tomu má schopnost a že třetí strana s přístupem k těmto údajům – na základě soudního příkazu, v důsledku narušení bezpečnosti nebo prodeje třetím stranám, pokud to podmínky služby umožňují – ji má také.

Přístup ke kontaktům

Další vektor, který prochází téměř bez povšimnutí: seznam kontaktů. Velká část messagingových služeb žádá při registraci o přístup k telefonnímu seznamu. Nahrají všechna čísla na svůj server, aby ukázaly, kdo další službu používá. Od té chvíle má společnost kompletní mapu vztahů uživatele, i když ten nikdy nikomu nenapsal jedinou zprávu.

Pro profesionála s profesním tajemstvím – právníka, lékaře, psychologa, poradce – tento seznam obsahuje klienty. Pokud byl seznam nahrán na server třetí strany, jména klientů jsou v infrastruktuře, jejíž jurisdikci a politiku profesionál nekontroluje. Profesní tajemství se neporuší v den, kdy někdo unikne konverzaci: bylo porušeno mnohem dříve, v okamžiku souhlasu s nahráním.

Rozdíl mezi šifrováním a nesbíráním

Šifrovat znamená chránit obsah. Být v soukromí znamená nesbírat to, co není potřeba. Jsou to odlišné věci a rozdíl je operativně kritický. Služba může všechny zprávy dokonale šifrovat a zároveň o svých uživatelích vědět téměř vše prostřednictvím metadat. Obě věci jsou dokonale kompatibilní. Ve skutečnosti je to dominantní obchodní model v odvětví.

Správná otázka pro posouzení skutečného soukromí služby nezní *"šifruje obsah?"*. Tato otázka je považována za zodpovězenou již léta. Správná otázka zní: *"jaká metadata generuje a kde se ukládají?"*. A především: *"jaká metadata nepotřebuje generovat?"*.

Architektura, která minimalizuje metadata záměrně (by design) – nikoli slibem, nikoli interní politikou – je strukturálně soukromější než architektura, která je sbírá a šifruje. Protože data, která neexistují, nelze uniknout, prodat, předat na základě soudního příkazu ani ztratit při narušení bezpečnosti.

Pro profesionálního čtenáře

Pokud vaše profesní činnost zahrnuje tajemství, důvěrnost nebo prostě respekt k informacím třetích stran, je vhodné si položit otázky v tomto pořadí:

1. Šifruje aplikace, kterou používám ke komunikaci, obsah? (Pravděpodobně ano.)
2. Šifruje metadata? (Pravděpodobně ne.)
3. Generuje metadata, která ke svému fungování *nepotřebuje*? (Téměř jistě ano.)
4. Kde jsou tato metadata uložena a pod jakou jurisdikcí? (Pravděpodobně mimo Evropský hospodářský prostor.)
5. Ví můj klient nebo pacient, že jsou tam jeho data?

Poslední otázka je ta nepříjemná. Protože upřímná odpověď ve většině případů zní, že ne.

Tento článek je první ze série o skutečném fungování profesionálních komunikačních nástrojů. Příští díly se budou věnovat souladu s GDPR v messagingu a konceptu profesního tajemství v digitální éře.

Zdroje a další čtení

- Hayden, M. – Prohlášení na Johns Hopkins University, 2014 ("We kill people based on metadata"). Veřejné přepisy k dispozici.
- GDPR (Nařízení EU 2016/679), čl. 4 a 5 – definice osobních údajů a zásady zpracování (metadata jsou osobní údaje).
- EDPS a EDPB – stanoviska k zpracování provozních údajů a metadat v elektronických komunikacích (směrnice ePrivacy).

← PředchozíStručná historie pečetního voskuDalší →Profesní tajemství v digitální éře

Nedávné čtení

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vezměte si tento článek tam, kam potřebujete.

↓ Markdown ↓ Prostý text ↓ PDF

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 e016c77b8a882fe2e941e21521c191dd59af3c4ab720a631097bc21791250302

Cuadernos Lacre · Publikace Menzuri Gestión S.L. ·
napsal R.Eugenio · rediguje tým Solo2.