Analiza · 16. svibnja 2026.

← Prethodno·Sljedeće →

Kada nema nikoga u sredini

Šifriranje onoga što prolazi kroz poslužitelj štiti sadržaj. Nemati poslužitelj u sredini eliminira to pitanje. Nije isto.

Dvije osobe, jedan razgovor

Kad dvije osobe razgovaraju licem u lice u sobi, nitko ne mora obećati da ništa nije čuo. Nije čuo jer ga nije bilo. Kada si dvoje ljudi dodaju papir iz jedne ruke u drugu, nitko u sredini ne mora prisegnuti da ga nije pročitao. Nema nikoga u sredini.

Većina stvari u svakodnevnom životu funkcionira ovako. Ne potpisujemo sporazume o povjerljivosti sa zrakom koji prenosi naš glas, niti s papirom koji držimo. Privatnost razgovora ne počiva na obećanju posrednika, jer posrednika nema. To je jedan od najjačih postojećih načina da se bude privatan: ne zato što se nešto ili netko dobro ponaša, već zato što ne postoji nešto ili netko.

Kada se razgovor preseli na digitalni kanal, to se prema zadanim postavkama mijenja. Uobičajeni model je sljedeći: dvije osobe se povežu na poslužitelj, poslužitelj primi poruku, šifrira je ili je spremi šifriranu, te je isporuči primatelju. Poslužitelj je u sredini. Poslužitelj može biti pošten. Može biti revidiran. Može djelovati u povoljnoj jurisdikciji i pod strogim pravilima o privatnosti. Sve to može biti istina. Ali poslužitelj je u sredini.

Razlika između šifriranja i neprikupljanja (drugi dio)

U prethodnom članku iz ove iste serije tvrdimo da šifriranje sadržaja i neprikupljanje metapodataka nisu ista stvar. Postoji još jedan korak koji treba jasno formulirati: šifriranje onoga što prolazi kroz poslužitelj i nemati poslužitelj također nisu ista stvar.

Prvi model — poslužitelj u sredini, šifrirani sadržaj — štiti sadržaj od operatera poslužitelja, njegovog osoblja za održavanje, od vanjskog napadača koji kompromitira sustav. I to je važno. Ali to ne eliminira poslužitelj. Poslužitelj je i dalje tamo. I dalje obrađuje metapodatke. To je i dalje točka koja može primiti sudski nalog, zakonsku intervenciju, politički pritisak ili kršenje sigurnosti. To je i dalje točka koja zahtijeva polaganje povjerenja u nekoga.

Drugi model — bez poslužitelja između dva kraja — ne štiti bolje šifrirani sadržaj: ako je kriptografija čvrsta, sadržaj je zaštićen u oba slučaja. Ono što se mijenja nije sadržaj. Ono što se mijenja jest da pitanje *»što je s poslužiteljem?«* više nema smisla, jer nema poslužitelja o kojem bi se moglo pitati.

Povjerenje, odsutnost i razlika između njih

Povjerenje može biti dobro položeno. Postoje poštene tvrtke. Postoje rigorozni revizori. Postoje zakoni povoljni za korisnike. Postoje ozbiljne usluge koje se strogo pridržavaju svega navedenog. Povjerenje, kada se ukaže operateru koji ga zaslužuje, nije loš dogovor.

Ali povjerenje, koliko god bilo čvrsto, ostaje povjerenje. To je društveno rješenje, a ne tehničko rješenje. Tvrtka može promijeniti vlasnika. Jurisdikcija može promijeniti vlast. Sudski nalog može stići sutra. Nova se ranjivost može otkriti sljedeći mjesec. Ništa se od ovoga ne događa iz loše namjere. Dogodi se jer operater postoji, a sve što postoji podložno je nepredviđenim situacijama svijeta.

Odsutnost operatera nije podložna istim tim nepredviđenim situacijama. Sudski nalog ne može tražiti podatke od poslužitelja koji ne postoji. Napadač ne može kompromitirati poslužitelj koji ne postoji. Promjena politike tvrtke ne može utjecati na podatke koje ta tvrtka nikada nije imala. Ključna fraza je jednostavna: podaci koji ne postoje ne mogu se izgubiti.

O legitimnom argumentu na strani poslužitelja

Tko god nudi profesionalnu uslugu razmjene poruka s poslužiteljem u sredini, obično formulira tri savršeno valjana argumenta. Prvo, da je poslužitelj neophodan kako bi zajamčio isporuku kada je primatelj izvan mreže. Drugo, da je šifriranje sadržaja snažno i stoga ga operater ne može čitati. Treće, da je usluga u skladu s europskim zakonodavstvom i da su podaci zaštićeni zakonom.

Sva tri argumenta su točna. Nijedan ne mijenja prirodu stvari. Istina je da poslužitelj omogućuje pohranu poruka za odgođenu isporuku; također je istina da se odgođena isporuka može riješiti na drugi način, pomoću protokola za izravnu komunikaciju između uređaja koji su poboljšavani desetljećima i operativni su danas. Istina je da je šifriranje sadržaja u tranzitu snažno u ozbiljnim uslugama. I istina je da europsko zakonodavstvo štiti korisnike više od onog u mnogim drugim mjestima.

Pitanje nije jesu li usluge s poslužiteljem u sredini legalne, niti jesu li sigurne, niti štite li sadržaj. Mogu biti, legalne su i obično su sigurne. Stvar je u tome da je postojanje poslužitelja u sredini arhitektonski izbor, a ne tehnička obveza. A svaki izbor ima posljedice. Arhitektura s poslužiteljem u sredini nužno stvara aktera kojem se mora vjerovati. Arhitektura bez poslužitelja u sredini ne.

Što zakon kaže, a što arhitektura radi

GDPR ne zahtijeva određeni arhitektonski model. Zahtijeva rezultate: smanjenje količine podataka, ograničenu svrhu, zaštitu integriranu u dizajn i prema zadanim postavkama, sposobnost demonstriranja sukladnosti. Usluga s poslužiteljem u sredini može ispuniti sve ove zahtjeve. Usluga bez poslužitelja u sredini ispunjava ih nekoliko po konstrukciji, a ne po deklaraciji. Apsolutno smanjenje — neprikupljanje ničega osim onoga što je strogo neophodno za isporuku poruke — trivijalno je kada ne postoji poslužitelj koji može nešto prikupiti.

Za svakodnevnu, neosjetljivu upotrebu, arhitektura poslužitelja sasvim je razumna, a povjerenje u ozbiljnog operatera vrijedeći je dogovor. Za druge namjene — one koje uključuju reguliranu profesionalnu tajnu, one koje podrazumijevaju deontološku odgovornost, one koje dotiču posebno osjetljive informacije — odsutnost točke povjerenja nije luksuz, to je strukturna prednost.

Za profesionalnog čitatelja

Pitanja koja treba postaviti kada se suočite s profesionalnom komunikacijskom uslugom, koja su nam već poznata iz prethodnih članaka u ovoj istoj seriji, nadopunjuju se samo još jednim arhitektonskim pitanjem:

1. Šifrira li sadržaj u tranzitu? (Vjerojatno da.)
2. Generira li i pohranjuje metapodatke o tome s kim razgovaram i kada? (Vjerojatno da.)
3. Postoji li poslužitelj na putu između mog uređaja i primateljevog?
4. Ako postoji: tko njime upravlja, u kojoj jurisdikciji i što bi se moralo dogoditi da preda podatke o meni?
5. Ako ne postoji: prethodna pitanja nemaju smisla.

Razlika između ove dvije kategorije nije u stupnju, već u vrsti. Kada dođe vrijeme da to objasnite klijentu, pacijentu ili kolegi, najiskrenija formulacija je također i najjednostavnija: u jednoj je netko u sredini; u drugoj, ne.

Ovaj članak zatvara početni ciklus Cuadernos Lacre. Nakon što smo razgovarali o šifriranju, metapodacima i profesionalnoj tajni, upotpunjujemo arhitektonsku sliku: šifriranje sadržaja i nemati poslužitelj u sredini su različite stvari. Obje mogu biti legalne; samo jedna eliminira točku povjerenja.

Izvori i dodatno štivo

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Temeljni tekst principa prema kojem jamstva sustava moraju biti implementirana na krajevima, a ne u posredničkom kanalu.
- Uredba (EU) 2016/679, čl. 25. — tehnička i integrirana zaštita podataka.
- Uredba (EU) 2016/679, čl. 5.1.c — načelo smanjenja količine podataka.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Poglavlja o arhitekturama koje po svojoj konstrukciji minimiziraju prikupljanje.

← PrethodnoGDPR i profesionalna razmjena poruka: zašto većina krši pravila, a da to i ne znaSljedeće →CUADERNOS_LIST_SCHREMS_TITLE

Nedavna čitanja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ponesite ovaj članak sa sobom gdje god vam zatreba.

↓ Markdown ↓ Obični tekst ↓ PDF

Datoteka će se preuzeti na vaš uređaj. Od tamo je možete spremiti, uvesti u Solo2 ili dijeliti gdje god želite. Cuadernos ne odlučuje o odredištu umjesto vas.

Voštani pečat · SHA-256 d598a488750a284834f68e7a2f537e6373ee885e570aa715c994a79c134b7f12

Cuadernos Lacre · Publikacija Menzuri Gestión S.L. ·
napisao R.Eugenio · uredio tim Solo2.