Keď v strede nikto nie je

Šifrovanie toho, čo prechádza cez server, chráni obsah. Absencia servera v strede eliminuje otázku. Nie je to to isté.

Dvaja ľudia, jeden rozhovor

Keď sa dvaja ľudia rozprávajú tvárou v tvár v miestnosti, nikto nemusí sľubovať, že nič nepočul. Nepočul, pretože tam nebol. Keď si dvaja ľudia podávajú papier z ruky do ruky, nikto v strede nemusí prisahať, že ho nečítal. V strede nikto nie je.

Väčšina vecí v každodennom živote funguje takto. Nepodpisujeme dohody o dôvernosti so vzduchom, ktorý prenáša náš hlas, ani s papierom, ktorý držíme. Súkromie rozhovoru nespočíva na sľube sprostredkovateľa, pretože neexistuje sprostredkovateľ. To je jedna z najsilnejších foriem súkromia: nie preto, že by sa niečo alebo niekto správal dobre, ale preto, že tam niečo alebo niekto nie je.

Keď sa rozhovor presunie do digitálneho kanála, toto sa predvolene mení. Zvyčajný model je nasledovný: dvaja ľudia sa pripoja k serveru, server prijme správu, zašifruje ju alebo ju uloží zašifrovanú a doručí ju príjemcovi. Server je v strede. Server môže byť čestný. Môže byť auditovaný. Môže pôsobiť v priaznivej jurisdikcii a podľa prísnych pravidiel ochrany súkromia. Toto všetko môže byť pravda. Ale server je v strede.

Rozdiel medzi šifrovaním a nezhromažďovaním (druhá časť)

V predchádzajúcom článku v tejto istej sérii tvrdíme, že šifrovanie obsahu a nezhromažďovanie metadát nie je to isté. Existuje ďalší krok, ktorý je vhodné jasne formulovať: šifrovanie toho, čo prechádza cez server, a absencia servera tiež nie je to isté.

Prvý model — server v strede, zašifrovaný obsah — chráni obsah pred operátorom servera, jeho personálom údržby, pred externým útočníkom, ktorý kompromituje systém. A to je dôležité. Ale neeliminuje server. Server je stále tam. Stále spracováva metadáta. Stále zostáva bodom, ktorý môže dostať súdny príkaz, zákonný zásah, politický tlak alebo únik dát. Stále zostáva bodom, ktorý vyžaduje zveriť niekomu dôveru.

Druhý model — absencia servera medzi oboma koncami — nechráni zašifrovaný obsah lepšie: ak je kryptografia solídna, obsah je chránený v oboch prípadoch. Čo sa mení, nie je obsah. Čo sa mení, je, že otázka *„čo je so serverom?“* prestáva mať predmet, pretože neexistuje server, na ktorý by sa bolo treba pýtať.

Dôvera, absencia a rozdiel medzi nimi

Dôvera môže byť dobre zverená. Čestné firmy existujú. Dôslední audítori existujú. Legislatívy priaznivé pre používateľov existujú. Seriózne služby, ktoré prísne dodržiavajú všetko uvedené, existujú. Dôvera, keď sa udelí operátorovi, ktorý si ju zaslúži, nie je zlé riešenie.

Ale dôvera, akokoľvek solídna, stále zostáva dôverou. Je to sociálne riešenie, nie technické. Firma môže zmeniť majiteľa. Jurisdikcia môže zmeniť vládu. Súdny príkaz môže prísť zajtra. Nová zraniteľnosť môže byť objavená budúci mesiac. Nič z toho sa nedeje v zlej viere. Deje sa to preto, že operátor existuje a všetko existujúce podlieha náhodám sveta.

Absencia operátora nepodlieha tým istým náhodám. Súdny príkaz nemôže žiadať dáta od servera, ktorý neexistuje. Útočník nemôže kompromitovať server, ktorý neexistuje. Zmena v politike firmy nemôže ovplyvniť dáta, ktoré tá firma nikdy nemala. Kľúčová veta je jednoduchá: dáta, ktoré neexistujú, sa nedajú stratiť.

O legitímnom argumente na strane servera

Kto ponúka profesionálnu službu správ so serverom v strede, zvyčajne formuluje tri dokonale platné argumenty. Po prvé, že server je potrebný na zaručenie doručenia, keď je príjemca odpojený. Po druhé, že šifrovanie obsahu je robustné, a preto ho operátor nemôže čítať. Po tretie, že služba dodržiava európsku legislatívu a že dáta sú chránené zákonom.

Všetky tri argumenty sú pravdivé. Žiadny nemení podstatu veci. Je pravda, že server umožňuje ukladať správy pre odložené doručenie; je tiež pravda, že odložené doručenie sa dá vyriešiť inak, prostredníctvom protokolov priamej komunikácie medzi zariadeniami, ktoré sa zdokonaľujú už desaťročia a fungujú dnes. Je pravda, že šifrovanie obsahu v tranzite je v seriózných službách robustné. A je pravda, že európska legislatíva chráni používateľov viac ako legislatíva mnohých iných miest.

Otázkou nie je, či sú služby so serverom v strede legálne, ani či sú bezpečné, ani či chránia obsah. Môžu nimi byť, sú legálne a zvyčajne sú bezpečné. Otázkou je, že mať server v strede je architektonická voľba, nie technické nanútenie. A každá voľba má následky. Architektúra so serverom v strede nevyhnutne vytvára aktéra, ktorému treba dôverovať. Architektúra bez servera v strede nie.

Čo hovorí zákon a čo robí architektúra

GDPR nevyžaduje konkrétny architektonický model. Vyžaduje výsledky: minimalizáciu dát, obmedzenie účelu, ochranu od dizajnu a predvolene, schopnosť preukázať súlad. Služba so serverom v strede môže spĺňať všetky tieto požiadavky. Služba bez servera v strede spĺňa viaceré z nich konštrukciou, nie deklaráciou. Absolútna minimalizácia — nezhromažďovať nič, čo nie je prísne potrebné na doručenie správy — je triviálna, keď neexistuje server, ktorý by mohol niečo zhromaždiť.

Pre každodenné necitlivé použitie je serverová architektúra dokonale rozumná a dôvera v seriózneho operátora je platným riešením. Pre ostatné použitia — tie, ktoré zahŕňajú regulované profesijné tajomstvo, tie, ktoré prinášajú deontologickú zodpovednosť, tie, ktoré sa dotýkajú obzvlášť citlivých informácií — absencia bodu dôvery nie je luxus, je to štrukturálna výhoda.

Pre profesionálneho čitateľa

Otázky, ktoré je vhodné si položiť pred profesionálnou komunikačnou službou, známe už z predchádzajúcich článkov v tejto istej sérii, dopĺňa ešte jedna architektonická otázka:

1. Šifruje obsah v tranzite? (Pravdepodobne áno.)
2. Generuje a ukladá metadáta o tom, s kým hovorím a kedy? (Pravdepodobne áno.)
3. Existuje server na ceste medzi mojím zariadením a zariadením príjemcu?
4. Ak existuje: kto ho operuje, v akej jurisdikcii a čo by sa muselo stať, aby odovzdal dáta o mne?
5. Ak neexistuje: predchádzajúce otázky nemajú predmet.

Rozdiel medzi týmito dvoma kategóriami nie je v stupni, ale v type. Keď príde čas vysvetliť to klientovi, pacientovi alebo kolegovi, najčestnejšia formulácia je zároveň tá najjednoduchšia: v jednej je niekto v strede; v

druhej nie.

Tento článok uzatvára úvodný cyklus Cuadernos Lacre. Po rozprávaní o šifrovaní, metadátach a profesijnom tajomstve dopĺňame architektonický obraz: šifrovanie obsahu a nemať server v strede sú rôzne veci. Obe môžu byť legálne; len jedna eliminuje bod dôvery.

Zdroje a ďalšie čítanie

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Zakladajúci text princípu, podľa ktorého sa záruky systému majú implementovať na koncoch, nie v sprostredkujúcom kanáli.
- Nariadenie (EÚ) 2016/679, čl. 25 — ochrana údajov už od návrhu a predvolená ochrana údajov.
- Nariadenie (EÚ) 2016/679, čl. 5.1.c — princíp minimalizácie údajov.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitoly o architektúrach, ktoré minimalizujú zber konštrukciou.

← PredchádzajúciGDPR a profesionálny messaging: prečo väčšina porušuje predpisy bez toho, aby o tom vedelaNasledujúci →CUADERNOS_LIST_SCHREMS_TITLE

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 acaeb9b8874a6158be4920de63aad86b6190a1535656fe2af8dbd01a6cf71e39

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