Analiza · 16. maja 2026

← Prejšnji·Naslednji →

Ko vmes ni nikogar

Šifriranje tistega, kar gre skozi strežnik, ščiti vsebino. Odsotnost strežnika vmes odpravi vprašanje. To ni isto.

Dva človeka, en pogovor

Ko se dva človeka pogovarjata iz oči v oči v sobi, nikomur ni treba obljubiti, da ni ničesar slišal. Ni slišal, ker ga ni bilo tam. Ko si dva človeka podata papir iz rok v roke, nikomur vmes ni treba priseči, da ga ni prebral. Vmes ni nikogar.

Večina stvari v vsakdanjem življenju deluje tako. Ne podpisujemo sporazumov o zaupnosti z zrakom, ki prenaša naš glas, niti s papirjem, ki ga držimo. Zasebnost pogovora ne sloni na obljubi posrednika, ker posrednika ni. To je eden najmočnejših načinov zasebnosti: ne zato, ker bi se nekaj ali nekdo dobro obnašal, temveč zato, ker nečesa ali nekoga ni.

Ko se pogovor preseli v digitalni kanal, se to privzeto spremeni. Običajni model je naslednji: dve osebi se povežeta s strežnikom, strežnik prejme sporočilo, ga šifrira ali shrani šifriranega in ga dostavi prejemniku. Strežnik je vmes. Strežnik je lahko pošten. Lahko je revidiran. Lahko deluje v ugodni jurisdikciji in pod strogo politiko zasebnosti. Vse to je lahko res. Toda strežnik je vmes.

Razlika med šifriranjem in nezbiranjem (drugi del)

V prejšnjem članku v tej isti seriji trdimo, da šifriranje vsebine in nezbiranje metapodatkov nista isto. Obstaja še korak naprej, ki ga je vredno jasno formulirati: šifriranje tistega, kar gre skozi strežnik, in odsotnost strežnika prav tako nista isto.

Prvi model — strežnik vmes, šifrirana vsebina — ščiti vsebino pred operaterjem strežnika, njegovim osebjem za vzdrževanje, pred zunanjim napadalcem, ki bi kompromitiral sistem. In to je pomembno. Toda ne odpravi strežnika. Strežnik je še vedno tam. Še naprej obdeluje metapodatke. Še vedno ostaja točka, ki lahko prejme sodni nalog, pravni poseg, politični pritisk ali vdor v varnost. Še vedno ostaja točka, ki zahteva zaupanje nekomu.

Drugi model — odsotnost strežnika med obema koncema — ne ščiti bolje šifrirane vsebine: če je kriptografija solidna, je vsebina zaščitena v obeh primerih. Kar se spremeni, ni vsebina. Kar se spremeni, je to, da vprašanje *»kaj se dogaja s strežnikom?«* izgubi predmet, ker ni strežnika, o katerem bi se spraševali.

Zaupanje, odsotnost in razlika med njima

Zaupanje je lahko dobro naloženo. Poštena podjetja obstajajo. Dosledni revizorji obstajajo. Zakonodaje, naklonjene uporabniku, obstajajo. Resne storitve, ki strogo izpolnjujejo vse zgoraj navedeno, obstajajo. Zaupanje, ko je podeljeno operaterju, ki si ga zasluži, ni slab dogovor.

Toda zaupanje, ne glede na to, kako solidno je, ostaja zaupanje. To je družbena rešitev, ne tehnična. Podjetje lahko zamenja lastnika. Jurisdikcija lahko zamenja vlado. Sodni nalog lahko pride jutri. Nova ranljivost se lahko odkrije prihodnji mesec. Nič od tega se ne zgodi v zli nameri. Zgodi se zato, ker operater obstaja, in vse, kar obstaja, je podvrženo naključjem sveta.

Odsotnost operaterja ni podvržena tem istim naključjem. Sodni nalog ne more zahtevati podatkov od strežnika, ki ne obstaja. Napadalec ne more kompromitirati strežnika, ki ne obstaja. Sprememba politike podjetja ne more vplivati na podatke, ki jih to podjetje nikoli ni imelo. Ključni stavek je preprost: podatkov, ki ne obstajajo, ni mogoče izgubiti.

O legitimnem argumentu na strane strežnika

Kdor ponuja profesionalno storitev sporočanja s strežnikom vmes, običajno formulira tri popolnoma veljavne argumente. Prvič, da je strežnik potreben za zagotavljanje dostave, ko je prejemnik odklopljen. Drugič, da je šifriranje vsebine robustno in zato operater ne more brati. Tretjič, da storitev izpolnjuje evropsko zakonodajo in da so podatki zaščiteni z zakonom.

Vsi trije argumenti so resnični. Noben ne spremeni narave zadeve. Res je, da strežnik omogoča shranjevanje sporočil za zapoznelo dostavo; res je tudi, da se zapoznela dostava lahko reši drugače, prek protokolov neposredne komunikacije med napravami, ki so se izpopolnjevali desetletja in delujejo danes. Res je, da je šifriranje vsebine v tranzitu robustno v resnih storitvah. In res je, da evropska zakonodaja ščiti uporabnike bolj kot tista v mnogih drugih krajih.

Vprašanje ni, ali so storitve s strežnikom vmes zakonite, niti ali so varne, niti ali ščitijo vsebino. Lahko so, so zakonite in so običajno varne. Vprašanje je, da je imeti strežnik vmes arhitekturna izbira, ne tehnična nujnost. In vsaka izbira ima posledice. Arhitektura s strežnikom vmes nujno ustvari akterja, ki mu je treba zaupati. Arhitektura brez strežnika vmes ne.

Kaj pravi zakon in kaj naredi arhitektura

Splošna uredba o varstvu podatkov (GDPR) ne zahteva določenega arhitekturnega modela. Zahteva rezultate: zmanjšanje količine podatkov, omejitev namena, zaščito s snovanjem in privzeto, sposobnost dokazovanja skladnosti. Storitev s strežnikom vmes lahko izpolnjuje vse te zahteve. Storitev brez strežnika vmes jih več izpolnjuje s konstrukcijo, ne z deklaracijo. Absolutno zmanjšanje — nezbiranje ničesar, kar ni nujno potrebno za dostavo sporočila — je trivialno, ko ni strežnika, ki bi lahko karkoli zbral.

Za vsakodnevne neobčutljive uporabe je strežniška arhitektura popolnoma razumna in zaupanje v resnega operaterja je veljaven dogovor. Za druge uporabe — tiste, ki vključujejo regulirano poklicno skrivnost, tiste, ki prinašajo deontološko odgovornost, tiste, ki se dotikajo posebej občutljivih informacij — odsotnost točke zaupanja ni luksuz, temveč strukturna prednost.

Za profesionalnega bralca

Vprašanja, ki si jih je vredno zastaviti pred profesionalno storitvijo komuniciranja, že znana iz prejšnjih člankov v tej isti seriji, se dopolnijo s še enim arhitekturnim vprašanjem:

1. Ali šifrira vsebino v tranzitu? (Verjetno da.)
2. Ali ustvarja in shranjuje metapodatke o tem, s kom govorim in kdaj? (Verjetno da.)
3. Ali obstaja strežnik na poti med mojo napravo in prejemnikovo?
4. Če obstaja: kdo ga upravlja, v kateri jurisdikciji in kaj bi se moralo zgoditi, da bi predal podatke o meni?
5. Če ne obstaja: prejšnja vprašanja nimajo predmeta.

Razlika med obema kategorijama ni v stopnji, temveč v vrsti. Ko pride čas, da to razložite stranki, pacientu ali kolegu, je najiskrenejša formulacija tudi najpreprostejša: v eni je nekdo vmes; v drugi ne.

Ta članek zaključuje začetni cikel Cuadernos Lacre. Po pogovoru o šifriranju, metapodatkih in poklicni skrivnosti dopolnjujemo arhitekturno sliko: šifriranje vsebine in odsotnost strežnika vmes sta različni stvari. Obe sta lahko zakoniti; le ena odpravi točko zaupanja.

Viri in nadaljnje branje

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Temeljno besedilo načela, po katerem se morajo jamstva sistema izvajati na koncih, ne v vmesnem kanalu.
- Uredba (EU) 2016/679, 25. člen — vgrajeno in privzeto varstvo podatkov.
- Uredba (EU) 2016/679, člen 5.1.c — načelo najmanjšega obsega podatkov.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Poglavja o arhitekturah, ki zmanjšujejo zbiranje s konstrukcijo.

← PrejšnjiGDPR in profesionalno sporočanje: zakaj večina krši pravila, ne da bi se tega zavedalaNaslednji →CUADERNOS_LIST_SCHREMS_TITLE

Zadnja branja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vzemite ta članek s seboj, kamor koli ga potrebujete.

↓ Markdown ↓ Navadno besedilo ↓ PDF

Datoteka bo prenesena v vašo napravo. Od tam jo lahko shranite, uvozite v Solo2 ali delite, kjer koli želite. Cuadernos ne odloča o cilju namesto vas.

Voščeni pečat · SHA-256 2cf2537e5a0b9309a65f371b987375607161ec45185029b9e2b4489c2e9f10e2

Cuadernos Lacre · Publikacija podjetja Menzuri Gestión S.L. ·
napisal R.Eugenio · uredila ekipa Solo2.