Analīze · 2026. gada 16. maijs

← Iepriekšējais · Nākamais →

Kad vidū neviena nav

Serverī nonākušā satura šifrēšana aizsargā pašu saturu. Servera trūkums vidū novērš pašu jautājumu. Tas nav viens un tas pats.

Divi cilvēki, viena saruna

Kad divi cilvēki istabā sarunājas aci pret aci, nevienam nav jāapsola, ka viņš neko nav dzirdējis. Viņš nedzirdēja, jo viņa tur nebija. Kad divi cilvēki nodod papīru no vienas rokas otrā, nevienam vidū nav jāzvēr, ka to nav lasījis. Vidū neviena nav.

Lielākā daļa lietu ikdienā darbojas tieši šādi. Mēs neparakstām konfidencialitātes līgumus ar gaisu, kas pārraida mūsu balsi, vai ar papīru, ko turam rokās. Sarunas privātums nebalstās uz starpnieka solījumu, jo starpnieka nav. Tas ir viens no spēcīgākajiem veidiem, kā būt privātam: nevis tāpēc, ka kaut kas vai kāds uzvedas labi, bet gan tāpēc, ka tur nekā un neviena nav.

Kad saruna pāriet uz digitālo kanālu, pēc noklusējuma tas mainās. Parastais modelis ir šāds: divi cilvēki savienojas ar serveri, serveris saņem ziņojumu, šifrē to vai saglabā šifrētu, un nogādā saņēmējam. Serveris ir pa vidu. Serveris var būt godīgs. Tas var būt auditēts. Tas var darboties labvēlīgā jurisdikcijā saskaņā ar stingru privātuma politiku. Tas viss var būt patiesība. Taču serveris ir pa vidu.

Atšķirība starp šifrēšanu un neievākšanu (otrā daļa)

Iepriekšējā šīs pašas sērijas rakstā mēs apgalvojam, ka satura šifrēšana un metadatu neievākšana nav viens un tas pats. Ir vēl viens solis, kas būtu skaidri jāformulē: tā šifrēšana, kas iet caur serveri, un servera neesamība arī nav viens un tas pats.

Pirmais modelis — serveris pa vidu, saturs šifrēts — aizsargā saturu no servera operatora, tā tehniskās apkopes personāla, no ārēja uzbrucēja, kas kompromitē sistēmu. Un tas ir svarīgi. Bet tas neizslēdz serveri. Serveris joprojām ir tur. Tas joprojām apstrādā metadatus. Tas joprojām ir punkts, kas var saņemt tiesas rīkojumu, juridisku iejaukšanos, izjust politisko spiedienu vai drošības pārkāpumu. Tas joprojām ir punkts, kurā kādam ir jāuzticas.

Otrais modelis — nav servera starp abiem galiem — neaizsargā šifrēto saturu labāk: ja kriptografija ir spēcīga, saturs abos gadījumos tiek aizsargāts. Mainās nevis saturs. Mainās tas, ka jautājums *„kas notiek ar serveri?”* zaudē nozīmi, jo nav servera, par kuru varētu jautāt.

Uzticēšanās, prombūtne un atšķirība starp tām

Uzticēšanās var būt labi pamatota. Pastāv godīgi uzņēmumi. Pastāv stingri auditori. Lietotājam labvēlīgi tiesību akti pastāv. Nopietni pakalpojumi, kas rūpīgi atbilst visiem iepriekš minētajiem, pastāv. Uzticēšanās, ja tā tiek piešķirta operatoram, kurš to ir pelnījis, nav slikts risinājums.

Tomēr uzticēšanās, lai cik tā būtu spēcīga, joprojām ir uzticēšanās. Tas ir sociāls risinājums, nevis tehnisks risinājums. Uzņēmums var mainīt īpašnieku. Jurisdikcija var mainīt valdību. Tiesas rīkojums var tikt izdots rīt. Jaunu ievainojamību var atklāt nākamnedēļ. Nekas no tā nenotiek sliktas gribas dēļ. Tas notiek tāpēc, ka operators eksistē, un viss, kas eksistē, ir pakļauts pasaules nejaušībām.

Operatora neesamība nav pakļauta šīm pašām nejaušībām. Tiesas rīkojums nevar pieprasīt datus no servera, kura nav. Uzbrucējs nevar kompromitēt serveri, kura nav. Uzņēmuma politikas izmaiņas nevar ietekmēt datus, kuru šim uzņēmumam nekad nav bijis. Galvenā frāze ir vienkārša: datus, kas neeksistē, nevar pazaudēt.

Par leģitīmo servera puses argumentu

Ikviens, kas piedāvā profesionālu ziņapmaiņas pakalpojumu ar serveri pa vidu, parasti formulē trīs pilnīgi pamatotus argumentus. Pirmkārt, serveris ir nepieciešams, lai nodrošinātu piegādi, kad saņēmējs ir bezsaistē. Otrkārt, satura šifrēšana ir spēcīga, un tādēļ operators to nevar izlasīt. Treškārt, pakalpojums atbilst Eiropas tiesību aktiem un datus aizsargā likums.

Visi trīs argumenti ir patiesi. Neviens nemaina lietas būtību. Tā ir taisnība, ka serveris ļauj saglabāt ziņojumus aizkavētai piegādei; ir arī taisnība, ka aizkavētu piegādi var atrisināt citādi, izmantojot tiešās saziņas protokolus starp ierīcēm, kas ir pilnveidoti gadu desmitiem un darbojas jau šodien. Tiesa, pārraides satura šifrēšana nopietnos pakalpojumos ir spēcīga. Un taisnība, ka Eiropas tiesību akti aizsargā lietotājus labāk nekā daudzās citās vietās.

Jautājums nav par to, vai pakalpojumi ar serveri pa vidu ir legāli, droši vai aizsargā saturu. Tie tādi var būt, ir legāli un parasti droši. Jautājums ir tāds, ka serveris pa vidu ir arhitektūras izvēle, nevis tehniska prasība. Un katrai izvēlei ir sekas. Arhitektūra ar serveri pa vidu neizbēgami rada spēlētāju, kuram ir jāuzticas. Arhitektūra bez servera pa vidu to nedara.

Ko saka likums, un ko dara arhitektūra

VDAR neprasa konkrētu arhitektūras modeli. Tas prasa rezultātus: datu minimizēšanu, mērķa ierobežojumu, integrētu datu apstrādes aizsardzību un aizsardzību pēc noklusējuma, spēju pierādīt atbilstību. Pakalpojums ar serveri pa vidu var izpildīt visas šīs prasības. Pakalpojums bez servera pa vidu atbilst vairākām no tām pēc konstrukcijas, nevis pēc deklarācijas. Absolūta minimizācija — nevākt neko, kas nav stingri nepieciešams ziņojuma piegādei — ir triviāla, ja nav servera, kas varētu kaut ko savākt.

Ikdienas, ne pārāk sensitīvai lietošanai arhitektūra ar serveri ir pilnīgi saprātīga, un uzticēšanās nopietnam operatoram ir derīgs risinājums. Citiem lietojumiem — tiem, kas saistīti ar regulētu profesionālo noslēpumu, tiem, kas ietver deontoloģisko atbildību, tiem, kas skar īpaši jutīgu informāciju — uzticības punkta neesamība nav luksuss, bet gan strukturāla priekšrocība.

Profesionālam lasītājam

Jautājumi, kas būtu jāuzdod, saskaroties ar profesionāliem komunikācijas pakalpojumiem un kas jau pazīstami no iepriekšējiem šīs sērijas rakstiem, tiek papildināti ar vēl vienu arhitektūras jautājumu:

1. Vai tas šifrē saturu pārsūtīšanas laikā? (Droši vien, ka jā.)
2. Vai tas ģenerē un saglabā metadatus par to, ar ko es runāju un kad? (Droši vien, ka jā.)
3. Vai starp manu un saņēmēja ierīci ir serveris?
4. Ja pastāv: kas to pārvalda, kādā jurisdikcijā, un kam būtu jānotiek, lai viņi varētu nodot datus par mani?
5. Ja tas nepastāv: iepriekšējiem jautājumiem nav nozīmes.

Atšķirība starp abām kategorijām ir nevis pakāpē, bet gan veidā. Kad pienāk laiks to izskaidrot klientam, pacientam vai kolēģim, godīgākais formulējums ir arī vienkāršākais: vienā no tiem kāds ir pa vidu; otrā — nav.

Šis raksts noslēdz Cuadernos Lacre sākotnējo ciklu. Pēc sarunām par šifrēšanu, metadatiem un profesionālo noslēpumu, mēs pabeidzam arhitektūras ainu: satura šifrēšana un servera neesamība ir divas dažādas lietas. Abas var būt legālas; tikai viena no tām izslēdz uzticības punktu.

Avoti un papildu literatūra

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Pamatteksts par principu, ka sistēmas garantijas ir jāīsteno galapunktos, nevis starpkanālā.
- Regula (ES) 2016/679, 25. pants — integrēta datu apstrādes aizsardzība un aizsardzība pēc noklusējuma.
- Regula (ES) 2016/679, 5. panta 1. punkta c) apakšpunkts — datu minimizēšanas princips.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Nodaļas par arhitektūrām, kas samazina ievākšanu pēc savas konstrukcijas.

← IepriekšējaisVDAR un profesionālā ziņapmaiņa: kāpēc vairums pārkāpj noteikumus, paši to nezinotNākamais →CUADERNOS_LIST_SCHREMS_TITLE

Jaunākie lasījumi

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Paņemiet šo rakstu līdzi tur, kur jums nepieciešams.

↓ Markdown ↓ Parasts teksts ↓ PDF

Fails tiks lejupielādēts jūsu ierīcē. No turienes varat to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi jūsu vietā.

Vaska zīmogs · SHA-256 a97b4f8117889607c852545499af323968e207e64cd4c14f08847ca44708696d

Cuadernos Lacre · Menzuri Gestión S.L. publikācija ·
autors R.Eugenio · rediģējusi Solo2 komanda.