Analizė · 2026 m. gegužės 16 d.

← Ankstesnis·Kitas →

Kai viduryje nieko nėra

Per serverį einančios informacijos šifravimas apsaugo turinį. Serverio nebuvimas viduryje panaikina patį klausimą. Tai nėra tas pats.

Du žmonės, vienas pokalbis

Kai du žmonės kalbasi akis į akį kambaryje, niekam nereikia žadėti, kad nieko negirdėjo. Negirdėjo, nes ten nebuvo. Kai du žmonės paduoda popierių vienas kitam, niekam viduryje nereikia prisiekti, kad jo neskaitė. Viduryje nieko nėra.

Dauguma dalykų kasdieniame gyvenime veikia būtent taip. Mes nepasirašome konfidencialumo sutarčių su oru, kuris perduoda mūsų balsą, ar su popieriumi, kurį laikome. Pokalbio privatumas nesiremia tarpininko pažadu, nes nėra jokio tarpininko. Tai yra viena stipriausių privataus buvimo formų: ne todėl, kad kažkas ar kažkas gerai elgiasi, o todėl, kad to kažko ar kažko paprasčiausiai nėra.

Kai pokalbis perkeliamas į skaitmeninį kanalą, tai pagal nutylėjimą pasikeičia. Įprastas modelis yra toks: du žmonės prisijungia prie serverio, serveris gauna pranešimą, jį užšifruoja arba išsaugo užšifruotą, ir pristato jį gavėjui. Serveris yra viduryje. Serveris gali būti sąžiningas. Jis gali būti audituojamas. Jis gali veikti palankioje jurisdikcijoje ir laikytis griežtos privatumo politikos. Visa tai gali būti tiesa. Tačiau serveris yra viduryje.

Skirtumas tarp šifravimo ir nerinkimo (antra dalis)

Ankstesniame šios pačios serijos straipsnyje teigiame, kad turinio šifravimas ir metaduomenų nerinkimas nėra tas pats. Yra dar vienas žingsnis, kurį reikėtų aiškiai suformuluoti: tai, kas praeina per serverį, užšifravimas ir serverio neturėjimas taip pat nėra tas pats.

Pirmasis modelis — serveris viduryje, turinys užšifruotas — apsaugo turinį nuo serverio operatoriaus, nuo jo priežiūros personalo, nuo išorinio užpuoliko, galinčio pažeisti sistemą. Ir tai yra svarbu. Tačiau tai nepanaikina serverio. Serveris vis dar ten. Jis vis dar apdoroja metaduomenis. Jis vis dar yra taškas, kuris gali gauti teismo reikalavimą, teisinę intervenciją, patirti politinį spaudimą ar saugumo pažeidimą. Jis vis dar yra taškas, reikalaujantis pasitikėjimo kažkuo.

Antrasis modelis — serverio nebuvimas tarp dviejų galų — neapsaugo užšifruoto turinio geriau: jei kriptografija tvirta, turinys yra apsaugotas abiem atvejais. Kas keičiasi, tai ne turinys. Keičiasi tai, kad klausimas *„kas nutiks su serveriu?“* netenka prasmės, nes nebelieka serverio, apie kurį būtų galima paklausti.

Pasitikėjimas, nebuvimas ir skirtumas tarp jų

Pasitikėjimas gali būti gerai pagrįstas. Sąžiningos įmonės egzistuoja. Griežti auditoriai egzistuoja. Vartotojui palankūs teisės aktai egzistuoja. Rimtos paslaugos, kurios kruopščiai atitinka visus šiuos reikalavimus, egzistuoja. Pasitikėjimas, kai jis suteikiamas operatoriui, kuris jo nusipelno, nėra blogas susitarimas.

Tačiau pasitikėjimas, koks jis bebūtų tvirtas, vis dar išlieka pasitikėjimu. Tai socialinis sprendimas, o ne techninis sprendimas. Įmonė gali pakeisti savininkus. Jurisdikcija gali pakeisti vyriausybę. Teismo įsakymas gali ateiti rytoj. Nauja pažeidžiamumo spraga gali būti atrasta kitą mėnesį. Niekas iš to nevyksta dėl blogos valios. Tai vyksta todėl, kad operatorius egzistuoja, ir viskas, kas egzistuoja, priklauso nuo pasaulio nenumatytų aplinkybių.

Operatoriaus nebuvimas nepriklauso nuo tų pačių aplinkybių. Teismo įsakymas negali prašyti duomenų iš serverio, kurio nėra. Užpuolikas negali kompromituoti serverio, kurio nėra. Įmonės politikos pasikeitimas negali paveikti duomenų, kurių ta įmonė niekada neturėjo. Pagrindinė frazė yra paprasta: duomenų, kurie neegzistuoja, neįmanoma prarasti.

Apie teisėtą serverio pusės argumentą

Tas, kas siūlo profesionalią pranešimų paslaugą su serveriu viduryje, paprastai pateikia tris visiškai pagrįstus argumentus. Pirma, serveris būtinas norint užtikrinti pristatymą, kai gavėjas yra atsijungęs. Antra, turinio šifravimas yra tvirtas, todėl operatorius negali jo perskaityti. Trečia, paslauga atitinka Europos teisės aktus, o duomenis saugo įstatymas.

Visi trys argumentai yra teisingi. Nė vienas iš jų nekeičia reikalo esmės. Tiesa, kad serveris leidžia saugoti pranešimus atidėtam pristatymui; taip pat tiesa, kad atidėtas pristatymas gali būti išspręstas kitu būdu, naudojant tiesioginio bendravimo tarp įrenginių protokolus, tobulinamus jau dešimtmečius ir veikiančius šiandien. Tiesa, kad perkeliamo turinio šifravimas yra tvirtas rimtose paslaugose. Ir tiesa, kad Europos teisės aktai saugo vartotojus labiau nei daugelyje kitų vietų.

Klausimas ne tame, ar paslaugos su serveriu viduryje yra legalios, ar saugios, ar jos apsaugo turinį. Jos gali tokios būti, yra legalios ir paprastai saugios. Klausimas tas, kad turėti serverį viduryje yra architektūrinis pasirinkimas, o ne techninė prievolė. Ir kiekvienas pasirinkimas turi pasekmių. Architektūra su serveriu viduryje neišvengiamai sukuria aktorių, kuriuo reikia pasitikėti. Architektūra be serverio viduryje to nedaro.

Ką sako įstatymas ir ką daro architektūra

BDAR nereikalauja konkretaus architektūrinio modelio. Jis reikalauja rezultatų: duomenų minimizavimo, tikslo apribojimo, pritaikytosios ir standartinės duomenų apsaugos, gebėjimo įrodyti atitiktį. Paslauga su serveriu viduryje gali atitikti visus šiuos reikalavimus. Paslauga be serverio viduryje atitinka kelis iš jų pagal konstrukciją, o ne pagal deklaraciją. Visiškas minimizavimas — nerinkti nieko, kas nėra griežtai būtina pranešimui pristatyti — yra trivialus, kai nėra serverio, kuris galėtų ką nors rinkti.

Kasdieniams jautrumo nereikalaujantiems atvejams architektūra su serveriu yra visiškai pagrįsta, o pasitikėjimas rimtu operatoriumi yra galiojantis susitarimas. Kitiems atvejams — tiems, kurie apima reguliuojamą profesinę paslaptį, tiems, kurie susiję su deontologine atsakomybe, tiems, kurie liečia ypač jautrią informaciją — pasitikėjimo taško nebuvimas yra ne prabanga, o struktūrinis pranašumas.

Profesionaliam skaitytojui

Klausimus, kuriuos verta užduoti susidūrus su profesionalia komunikacijos paslauga, jau pažįstamus iš ankstesnių šios pačios serijos straipsnių, papildo dar vienas architektūrinis klausimas:

1. Ar turinys šifruojamas siuntimo metu? (Tikriausiai taip.)
2. Ar generuojami ir saugomi metaduomenys apie tai, su kuo ir kada aš kalbu? (Tikriausiai taip.)
3. Ar yra serveris kelyje tarp mano įrenginio ir gavėjo?
4. Jei yra: kas jį valdo, kokioje jurisdikcijoje ir kas turėtų įvykti, kad jie perduotų duomenis apie mane?
5. Jei nėra: ankstesni klausimai netenka prasmės.

Skirtumas tarp šių dviejų kategorijų yra ne laipsnio, o rūšies. Atėjus laikui paaiškinti tai klientui, pacientui ar kolegai, sąžiningiausia formuluotė taip pat yra pati paprasčiausia: vienu atveju kažkas yra viduryje; kitu atveju — ne.

Šis straipsnis užbaigia pradinį Cuadernos Lacre ciklą. Pakalbėję apie šifravimą, metaduomenis ir profesinę paslaptį, užbaigiame architektūrinį paveikslą: turinio šifravimas ir serverio nebuvimas viduryje yra skirtingi dalykai. Abu gali būti legalūs; tik vienas panaikina pasitikėjimo tašką.

Šaltiniai ir papildomas skaitymas

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Pamatinis principo tekstas, pagal kurį sistemos garantijos turi būti įgyvendinamos galuose, o ne tarpiniame kanale.
- Reglamentas (ES) 2016/679, 25 str. — pritaikytoji ir standartinė duomenų apsauga.
- Reglamentas (ES) 2016/679, 5 str. 1 d. c punktas — duomenų kiekio mažinimo principas.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Skyriai apie architektūras, kurios pagal konstrukciją sumažina duomenų rinkimą.

← AnkstesnisBDAR ir profesionalus susirašinėjimas: kodėl dauguma pažeidžia taisykles to nežinodamiKitas →CUADERNOS_LIST_SCHREMS_TITLE

Naujausi skaitiniai

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Pasiimkite šį straipsnį su savimi ten, kur jums reikia.

↓ Markdown ↓ Paprastas tekstas ↓ PDF

Failas bus atsisiųstas į jūsų įrenginį. Iš ten galite jį išsaugoti, importuoti į Solo2 arba bendrinti bet kur. Cuadernos nusprendžia ne jūsų naudai dėl paskirties vietos.

Vaško antspaudas · SHA-256 b496976ee0059b7b3a88a1e0dae5671e90cca8addc65ab0b75d74be07e2d3208

Cuadernos Lacre · Menzuri Gestión S.L. leidinys ·
parašė R.Eugenio · redagavo Solo2 komanda.